

Report Documentation Page			<i>Form Approved</i> <i>OMB No. 0704-0188</i>	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.				
1. REPORT DATE 18-06-10		2. REPORT TYPE Master's Thesis		3. DATES COVERED 27-07-09 to 18-06-10
4. TITLE AND SUBTITLE The Sensor Irony: How Reliance on Sensor Technology Is Limiting Our View of the Battlefield			5a. CONTRACT NUMBER	
			5b. GRANT NUMBER	
			5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR (S) Major Glen E. Clubb, U.S. Army			5d. PROJECT NUMBER	
			5e. TASK NUMBER	
			5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME (S) AND ADDRESS (ES) National Defense University, Joint Forces Staff College, 7800 Hampton Blvd, Norfolk, VA, 23511-1702			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME (S) AND ADDRESS (ES)			10. SPONSOR/MONITOR'S ACRONYM (S)	
			11. SPONSOR/MONITOR'S REPORT NUMBER (S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited				
13. SUPPLEMENTARY NOTES				
14. ABSTRACT <p>This study shows that Department of Defense (DOD) overdependence on air and space-based sensor technologies reduces the surveillance and reconnaissance (S&R) capability of the operational-level commander and sets the conditions for initial failure on the future battlefield.</p> <p>An analysis of DOD capability priorities from 1950 to present shows a steady increase in reliance on technological solutions coupled with reduced manpower. Within his vision of department-wide transformation, Secretary of Defense Donald Rumsfeld gave new impetus to this technological focus. Transformation, more than just improving capabilities, fundamentally changed how DOD viewed the conduct of war. Analysis shows that transformation was not necessarily a bad concept, but was flawed in its extreme interpretations and subsequent execution.</p> <p>Analyzing the capabilities and limitations of DOD's current and predicted S&R force reveals a wide disparity between ground and air/space-based systems. Further assessing these systems against battlefield constraints reveals an S&R force structure that, while functional in a permissive environment, will not perform as advertised against plausible future threat scenarios.</p> <p>Many potential adversaries currently possess the ability to negate U.S. S&R capabilities. While it is never too late to fix a problem, DOD must first acknowledge that a problem exists. Ground S&R assets, particularly at the Army Corps/Marine Expeditionary Force, and Army Division/Marine Expeditionary Brigade level, must return to time tested and historically justified capabilities if the U.S. is to avoid future mission failure or unnecessary loss of life and treasure.</p>				
15. SUBJECT TERMS ISR, Surveillance, Reconnaissance, Sensor, Transformation, Technology, Aerial, Space-based				
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Unclassified Unlimited	18. NUMBER OF PAGES 124
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified		

**JOINT FORCES STAFF COLLEGE
JOINT ADVANCED WARFIGHTING SCHOOL**

**THE SENSOR IRONY: HOW RELIANCE ON SENSOR TECHNOLOGY IS
LIMITING OUR VIEW OF THE BATTLEFIELD**

by

Glen E. Clubb

Major, United States Army



A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

This paper is entirely my own work except where documented in footnotes.

Signature: _____

10 May 2010

Thesis Advisor: James F. Dickens, COL, U.S. Army

ABSTRACT

This study shows that Department of Defense (DOD) overdependence on air and space-based sensor technologies reduces the surveillance and reconnaissance (S&R) capability of the operational-level commander and sets the conditions for initial failure on the future battlefield.

An analysis of DOD capability priorities from 1950 to present shows a steady increase in reliance on technological solutions coupled with reduced manpower. Within his vision of department-wide transformation, Secretary of Defense Donald Rumsfeld gave new impetus to this technological focus. Transformation, more than just improving capabilities, fundamentally changed how DOD viewed the conduct of war. Analysis shows that transformation was not necessarily a bad concept, but was flawed in its extreme interpretations and subsequent execution.

Analyzing the capabilities and limitations of DOD's current and predicted S&R force reveals a wide disparity between ground and air/space-based systems. Further assessing these systems against battlefield constraints reveals an S&R force structure that, while functional in a permissive environment, will not perform as advertised against plausible future threat scenarios.

Many potential adversaries currently possess the ability to negate U.S. S&R capabilities. While it is never too late to fix a problem, DOD must first acknowledge that a problem exists. Ground S&R assets, particularly at the Army Corps/Marine Expeditionary Force, and Army Division/Marine Expeditionary Brigade level, must return to time tested and historically justified capabilities if the U.S. is to avoid future mission failure or unnecessary loss of life and treasure.

ACKNOWLEDGEMENTS

I would like to thank COL James Dickens, Dr. Paul Melshen, Dr. Gail Nicula, and Dr. Bryon Greenwald for their candid feedback and continued guidance throughout this year-long adventure.

A special thank you goes to my wife, Tammy, my daughter, Allyson, and my son, Andrew, whose support proved invaluable. Tammy's ability to keep us all pointed in the right direction, Andrew's daily reminder to "make good grades and stay out of trouble," and Allyson's weekly offer to assist me with my "book" made the perpetual wire-brushing from COL Dickens seem that much better.

TABLE OF CONTENTS

ABSTRACT	i
ACKNOWLEDGEMENTS	ii
TABLE OF CONTENTS	iii
FIGURES.....	iv
TABLES.....	v
INTRODUCTION TO THE SENSOR IRONY	1
CHAPTER 1. SURVEILLANCE AND RECONNAISSANCE CAPABILITY	9
DOD S&R Capability Priorities.....	9
Projected S&R Capabilities	28
CHAPTER 2. CAPABILITIES GAP ON FUTURE BATTLEFIELDS.....	51
The Operational Environment.....	51
Sensor Allocation Criteria.....	61
Terrain Constraints.....	63
Weather Constraints.....	68
Threat Constraints	69
CHAPTER 3. CHINA: A THREAT CASE STUDY	72
CONCLUSION	77
APPENDIX A. OPERATIONAL INFORMATION REQUIREMENTS	80
Fundamental Concepts.....	80
Doctrinal Review	82
APPENDIX B. DOD TECHNOLOGY CONCEPTS	87
Revolution in Military Affairs	88
Network-Centric Warfare	91
Information Dominance	95
APPENDIX C. AIR/SPACE-BASED SYSTEM CAPABILITIES.....	99
BIBLIOGRAPHY	110
VITA.....	116

FIGURES

Figure 1: Intelligence Disciplines 2

Figure 2: Intelligence Process 7

Figure 3: USAF and USA Aerial/Space-Based S&R Assets 32

Figure 4: Satellite Orbits 38

Figure 5: Possible Ground S&R Assets Available to USSOCOM 45

Figure 6: Ground S&R Assets Available to USJFCOM 49

Figure 7: Asset Capability Factors 62

Figure 8: S&R Asset Comparison in Densely Wooded/Jungle Terrain 64

Figure 9: S&R Asset Comparison in Mountainous Terrain 66

Figure 10: S&R Asset Comparison in Urban Terrain 67

Figure 11: S&R Asset Comparison with Weather Constraints 68

Figure 12: S&R Asset Comparison with Threat Constraints 71

Figure 13: Levels of Intelligence 83

TABLES

Table 1: MQ-1 Predator (U.S. Army MQ-1C Sky Warrior) 100

Table 2: MQ-9 Reaper 101

Table 3: RQ-4 Global Hawk (U.S. Navy RQ-4N) 103

Table 4: MC-12 Liberty (U.S. Army MARSS) 104

Table 5: RC-135V/W Rivet Joint 105

Table 6: E8C Joint Surveillance Target Attack Radar System (JSTARS) 106

Table 7: U2S Dragon Lady 107

Table 8: Improved/Advanced Crystal, IKON, or KH-12 108

Table 9: Lacrosse, Onyx, Vega 108

Table 10: Mentor, Advanced Mentor, Advanced Orion 109

Table 11: Trumpet 109

Table 12: Mercury, Vortex-II, Advanced Vortex 109

CHAPTER 1

INTRODUCTION TO THE SENSOR IRONY

This study will show that Department of Defense (DOD) overdependence on air and space-based sensor technologies reduces the surveillance and reconnaissance (S&R) capability of the operational-level commander and sets the conditions for initial failure on the future battlefield. As stated in the 2006 Quadrennial Defense Review (QDR), “technological advances, including dramatic improvements in information management and precision weaponry, have allowed our military to generate considerably more combat capability ... with the same or, in some cases, fewer numbers of weapons platforms and with lower levels of manning.”¹ Couple these with advances in optics and communications and the U.S. has a far more capable S&R force than that of just a few years ago. However, consider the following from the 2010 Marja offensive in Afghanistan:

On the satellite photographs of Marja that Marines scrutinized before launching a massive assault against the Taliban a week ago, what they assumed was the municipal government center appeared to be a large, rectangular building, cater-cornered from the main police station. Seizing that intersection became a key objective, one deemed essential to imposing authority and beginning reconstruction in this part of Helmand province But when Marine officers reached the area, they discovered that two-dimensional images can be deceiving ... the flat

¹ Department of Defense, *Quadrennial Defense Review Report*, (Washington, D.C., 2006), v.

roof of the municipal building turned out to be a concrete foundation, and the police station was a bombed-out schoolhouse.²

In this case, technology-based S&R capabilities led to incorrect conclusions about the focus of military operations. Though this particular mistake was of little potential consequence, such a mistake might have proven quite costly in terms of resources expended, or misdirected maneuver and fires toward an irrelevant “key objective.” High-tech answers to our operational questions may not be as valuable as they might seem.

According to the DOD 2006 Quadrennial Defense Review (QDR), “the ability of the future force to establish an ‘unblinking eye’ over the battle-space through persistent surveillance will be key to conducting effective joint operations.”³ It goes on to say that “future capabilities in ISR [intelligence surveillance and reconnaissance], including those operating in space, will support operations against any target, day or night, in any weather, and in denied or contested areas.”⁴ With such an assertion of perceived future capabilities, it is ironic that the



Figure 1: Intelligence Disciplines

² Rajiv Chandrasekaran, “Offensive is Just the Beginning in Marja,” *The Washington Post*, February 21, 2010.

³ DOD, *Quadrennial Defense Review Report*, 55.

⁴ Ibid.

procurement of these very capabilities could in fact limit U.S. armed forces' effectiveness in S&R operations.

For many, it is difficult to see through this irony and comprehend the urgency of the issue. With decades of exponential growth in technology, today's commanders receive an unprecedented amount of information. Along with the litany of intelligence disciplines and sources listed in Figure 1, instantaneous voice and data communications link decision makers with nearly every asset in the arsenal; satellites to aircraft to ground maneuver forces. For Afghanistan and Iraq, these linkages were extended even to the individual serviceman where everyone on the battlefield worked as an independent sensor generating innumerable bits of information.⁵ At a glance it would seem that the commander has a near-perfect view of the battlefield. But while the latest in technological sensors are truly combat multipliers, the U.S. military may find itself lacking after the full accounting of cost-versus-benefit for many untested S&R technologies.

Military historian John L. Romjue wrote that "we are an Army historically unprepared for its first battle."⁶ Romjue's claim could easily refer to the military establishment as a whole as U.S. joint forces often demonstrate significant systemic

⁵ Director of National Intelligence McConnell said that "U.S. intelligence agencies will never have enough analysts to fully examine all the data they collect." Mike McConnell, "Overhauling Intelligence," *Foreign Affairs* (July/August 2007), 53.

⁶ John L. Romjue, *From Active Defense to AirLand Battle: The Development of Army Doctrine, 1973-1982*. (Fort Monroe: Historical Office, United States Army Training and Doctrine Command, 1984), 6.

weaknesses at the onset of modern crises. However, the U.S. armed forces learn quickly from initial mistakes, making both organizational and tactical adjustments applicable to the current situation. Thus, when discussing national-level resource allocation, the military becomes a victim of its own success. It overcomes capability gaps through the temporary compromise of U.S. interests and the commitment of American lives to gain enough time for the requisite organization and equipment changes to reach the battlefield. Just as in past conflicts, the U.S. armed forces will have to overcome future capability gaps while in contact with enemy forces.

The 2008 National Defense Strategy states that: “Implementation of any strategy is predicated on developing, maintaining and, where possible, expanding the means required to execute its objectives within budget constraints.”⁷ However, in all but the most extraordinary circumstances, military spending is a zero-sum gain. Meaning, unless Congress can be persuaded to increase the overall DOD budget, increasing funding to a particular program means DOD must reduce funding in another. As such, it is with some risk that the U.S. replaces historically-justified capabilities with unproven technology-based solutions.

Our prime weapon in our struggles with terrorists, insurgents, and warriors of every patchwork sort remains the Soldier or Marine; yet, confronted with reality’s bloody evidence, we simply pretend that

⁷ DOD, *The National Defense Strategy*, (Washington, D.C., 2008), 18.

other, future, hypothetical wars will justify the systems we adore – purchased at the expense of the assets we need.⁸

In essence, the U.S.'s historic preoccupation with technological solutions can severely limit the effectiveness of their prime collection system – the American fighting man.

Technology is not inherently detrimental to military operations; quite the contrary. “History is littered with prophecies of technical and scientific inadequacy, such as Lord Kelvin’s famous retort, ‘Heavier-than-air flying machines are impossible.’”⁹ Discussions on the possibility of spaceflight fell in a similar vein. “A *New York Times* editorial in 1921 ... excoriated Robert Goddard for his silly notions of rocket-propelled space exploration Compounding its error in judgment, in 1936, the *Times* stated flatly, ‘A rocket will never be able to leave the Earth’s atmosphere.’”¹⁰ Many new technologies will outperform the predictions of their original detractors. In fact, America enjoys a history of innovation and the DOD is often at the cutting edge of new developments. However, the department should strive to maintain this pattern of success while ensuring the force remains capable across the full-spectrum of conflict.

⁸ Ralph Peters, "The Counterrevolution in Military Affairs: Fashionable Thinking about Defense Technology Ignores the Great Threats of Our Time," *The Weekly Standard*, 6 February 2006, 18.

⁹ Everett C. Dolman, "A Debate About Weapons in Space: For U.S. Military Transformation and Weapons in Space," *SAIS Review* (2006), 168. Lord Kelvin was a leading physicist and then president of the Royal Society in 1895.

¹⁰ Ibid.

Joint doctrine provides little by way of operational guidance should it lose, for any extended period of time, digital network connectivity, Global Positioning System (GPS) satellite coverage, platform data links, etc. Thus, DOD leadership seems to assume that it will always have use of this technological backbone and, by extension, its aerial and space-based S&R systems. This may be a mistake. That said, the technical vulnerabilities of the U.S. network backbone exceed the parameters of this unclassified study. As such, this issue will only be discussed in the most general terms. Nonetheless, as an underlying principle, this paper assumes that, despite scores of experts working to protect existing capabilities, enemy forces may still find ways to diminish U.S. network effectiveness, and thereby marginalize any technology-based advantage.

This study compares operational commander information needs against fielded and future collection assets. Beginning with the evolution of DOD S&R capability priorities and ending with a detailed study of S&R assets, the first chapter provides an itemized list of predicted S&R capabilities which assumes no change to current procurement trends. These capabilities are then analyzed across the spectrum of plausible battlefield conditions, thus highlighting predicted capability gaps with reference to commander information needs, asset requirements, and the fundamentals of

reconnaissance.¹¹ This is followed by a brief case study in Chinese military intent and capabilities. The case study provides a real-world backdrop to view the capability gaps of the preceding chapter.

As a pre-requisite, the reader should have an intimate knowledge of the operational level of war as well as the 1980/90s DOD concepts of the “Revolution in Military Affairs” (RMA), Net-Centric Warfare (NCW), and Information Dominance/Dominant Battlefield Awareness.¹²

It is assumed that the operational commander will begin operations with some

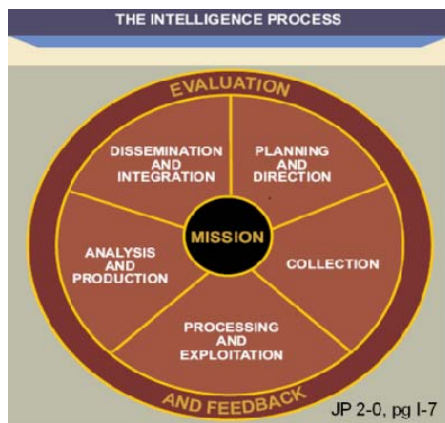


Figure 2: Intelligence Process

degree of synthesized intelligence from the various intelligence agencies. As such, this analysis focuses primarily on the collection portion of the intelligence cycle depicted in Figure 2. Further, this study does not discuss the non-DOD elements of national power, non-governmental organizations (NGOs), or support organizations within the DOD.

¹¹ According to *U.S. Army Field Manual 3-90*, the Fundamentals of Reconnaissance are: ensure continuous reconnaissance, do not keep reconnaissance assets in reserve, orient on the reconnaissance objective, report information rapidly and accurately, retain freedom of maneuver, gain and maintain enemy contact, and develop the situation rapidly. Headquarters, Department of the Army, *Field Manual 3-90, Tactics*, (Washington, D.C., 2001), 13-1.

¹² Appendices A and B provide background information on these subjects.

At the conclusion of this study, the reader will have a fundamental understanding of the sensor irony facing both the DOD leadership and operational commanders. Through critical analysis, the current and predicted reliance on aerial and space-based S&R will be shown to be both dangerous and misguided in light of the threat possibilities. As stated previously, the U.S. is not risking loss of a war, but could save itself considerable loss in manpower and resources by correcting current S&R trends.

CHAPTER 2

SURVEILLANCE AND RECONNAISSANCE CAPABILITY

This chapter begins with an outline of the DOD S&R capability priorities. These priorities provide insight into the genesis and evolution of S&R capabilities from the 1950s through the present. The second half of this chapter describes the collection assets that will be available to the operational commander for the perceivable future as predicted by the S&R trends.

DOD S&R Capability Priorities

Cold War to Operation Desert Storm

Marine Corps Colonel James Howcroft¹ wrote that during the Cold War arms race with the Soviet Union, strategic and national level objectives were seen as key to gaining victory over communist conventional armed forces. Targets “were generally static sites, such as headquarters, missile silos, airfields, or railroad marshalling yards. Intelligence collection was prioritized to provide accurate targeting data and follow-on bomb damage assessment ... for manned and unmanned airborne weapons.”² The information needs of ground-based tactical and operational level commanders “were only of secondary importance; units at this level were not critical to success. Victory was won

¹ Colonel Howcroft is the military professor of international security studies at the George C. Marshall Center for European Security Studies.

² James R. Howcroft, "Technology, Intelligence, and Trust," *Joint Forces Quarterly*, no. 46 (3rd Quarter 2007), 20.

or lost at the strategic level.”³ DOD’s acquisition of intelligence assets thus focused on building capabilities to monitor strategic targets, primarily in peacetime conditions.

With a focus on strategic targets and a desire to curtail defense spending, U.S. leadership sought to reap savings through reduced military manpower. Author and University of Wisconsin-Madison political science professor, David W. Tarr, wrote that the United States “clung to the hope throughout the 1950s that it could exploit its presumed technological superiority to reap significant political, economic, and military dividends.”⁴ One expected outcome of the U.S. technological superiority was an ability to reduce manpower across the department, particularly in the ground combat and reconnaissance forces. However, “its technology failed to bear the expected fruit ... the sophisticated machinery of warfare did not always prove superior to manpower; and often, rather than supplanting manpower, it created new requirements for it.”⁵

Historian and scholar Michael Ignatieff said that this trend continued even after the end of the Cold War. “The new military technology seemed to offer politicians a way to cut back defense budgets without reducing military preparedness, by increasing the

³ Ibid.

⁴ David W. Tarr, *American Strategy in the Nuclear Age* (New York: Macmillan Publishing Co., Inc, 1966), 69.

⁵ Ibid.

lethality of the military machine while sharply reducing its size and cost. In the decade after 1989, the American armed services shed 36 percent of their personnel.”⁶

This loss of personnel and focus on technology was seemingly justified when the American military put its might on display in Operation Desert Shield/Storm. It is only in hindsight that the U.S. realized that its high-tech suite of S&R capability did not provide operational decision-makers with an accurate depiction of Iraqi forces. Despite this, “the Department of Defense, reinforced by the stunning success of advanced weaponry in the Gulf War, quickly gravitated to a high-tech version of war. After all, it played to the strength the United States had used to defeat both the Soviet Union and Iraq.”⁷

This strategic focus for high technology coupled with reduced military manpower pervaded defense procurement priorities when Donald Rumsfeld returned as Secretary of Defense in 2001.⁸

Secretary Rumsfeld S&R Priorities

Under Rumsfeld’s new leadership, DOD initiated a shift away from threat-based planning and toward capabilities-based planning, and in so doing changed “the way war-fighting needs are defined and prioritized.”⁹ Capabilities-based planning sought to “identify capabilities that adversaries could employ and capabilities that could be

⁶ Michael Ignatieff, *Virtual War, Kosovo and Beyond* (New York: Picador USA, 2000), 172.

⁷ Thomas X. Hammes, *The Sling and the Stone: On War in the 21st Century* (St. Paul: Zenith Press, 2006), 6.

⁸ Donald Rumsfeld also served as Secretary of Defense from 1975-1977.

⁹ DOD, *Quadrennial Defense Review Report*, 4.

available to the United States, then evaluate their interaction, rather than over-optimize the joint force for a limited set of threat scenarios.”¹⁰ This paradigmatic shift in how defense capabilities were justified moved the department towards a more well-rounded approach to resourcing the military’s role in several possible contingencies as opposed to a myopic approach to the defense of Europe and Korea. This also prompted a shift away from strategic targeting toward a renewed focus on the operational needs of the Combatant Commanders “as the basis for programs and budgetary priorities.”¹¹ These were both positive moves that sought to maintain relevancy and agility across the department.

Clay Risen, assistant editor for *The New Republic*, said that “Rumsfeld’s business revolution is changing more than the way the military is structured; it is altering the very way war is fought Rumsfeld has argued that the U.S. Armed Forces are so technologically advanced that traditional doctrine – and thousands of years of military history – are largely irrelevant.”¹² With specific reference to the S&R community, Rumsfeld was an architect and advocate for the current Revolution in Military Affairs (RMA), Network-Centric Warfare (NCW), and Information Dominance.¹³ This section

¹⁰ Ibid.

¹¹ Ibid.

¹² Clay Risen, "War-Mart: the danger of generals-as-CEOs," *The New Republic*, April 3, 2006, 20.

¹³ Thomas X. Hammes, *The Sling and the Stone*, 6.

of the paper will build upon those concepts and show how they affected S&R capability priorities.

The 2004 National Military Strategy states that the goal of the joint force is “full spectrum dominance – the ability to control any situation or defeat any adversary across the range of military operations.”¹⁴ Achieving full spectrum dominance and the “qualitative military advantages the United States enjoys today will require transformation - a transformation achieved by combining technology, intellect and cultural changes across the joint community.”¹⁵

Leading DOD’s transformation efforts was Admiral Arthur Cebrowski, director of the Office of Force Transformation, an office created by Secretary Rumsfeld in 2001. Admiral Cebrowski viewed the strategic environment and U.S. overmatch in capabilities such that the transformation to a capabilities-based force meant removal of “legacy systems, doctrines, and processes ... if we pay for the new by relinquishing the old – as we should and are likely to do – it will not only go faster, but will accelerate.”¹⁶ He said that military capabilities designed to address traditional threats “will simply be moved off the table. Now we expect to justify systems based on their capabilities against irregular or

¹⁴ DOD, *The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow*, (Washington, D.C., 2004), 23.

¹⁵ *Ibid.*, viii.

¹⁶ Arthur Cebrowski, "Transforming Transformation," *Transformation Trends*, April 19, 2004, 9.

catastrophic challenges – the degree of capability proved against traditional challenges will be the added benefit.”¹⁷

Under Rumsfeld’s and Cebrowski’s vision, DOD needed to move away from outdated conventional warfighting capabilities. But how did it plan to do this? Five years later, the 2006 QDR showed that the department had shifted from “an emphasis on ships, guns, tanks and planes – to focus on information, knowledge and timely, actionable intelligence.”¹⁸ Admiral Cebrowski summarized this point at the 2003 Network Centric Warfare conference:

When we put this all together we see that a new American way of war is emerging ... you have to do something decidedly different and that thing that is different is the substitution of information for mass. Organizational structures are going to change ... a lot of lines have to disappear off the map and off the organizational charts.¹⁹

Thus the U.S. no longer needed to emphasize a ground-based S&R force that could fight for information, because traditional threats were no longer a main concern. As such, the military could reallocate its resources toward more lucrative capabilities.

Consistent with Rumsfeld’s and Cebrowski’s vision, DOD reductions in manpower and traditional systems led to a number of S&R initiatives. While even a cursory description of each initiative is outside the scope of this paper, they fall into five

¹⁷ Ibid., 5.

¹⁸ DOD, *Quadrennial Defense Review Report*, vi-vii.

¹⁹ Arthur Cebrowski, "Speech to the Network Centric Warfare 2003 Conference," *Center for Defense Information, Military Reform Project*; available from <http://www.cdi.org/mrp/tt-17feb03.pdf>; Internet; accessed 15 October 2009.

general categories: maintain a technological advantage over potential adversaries, gain decision superiority, achieve persistent surveillance capability, maintain dominance in space-based operations, and increase special operations forces (SOF). As will be established in the next chapter, this relative shift away from consideration of traditional threats and removal of the systems required to function against them created a number of S&R capability gaps.

It has been, will always be, and should always be the goal of the United States military to maintain technological superiority over potential adversaries. “Sustaining America’s scientific and technological advantages over any potential competitor contributes to the nation’s ability to dissuade future forms of military competition.”²⁰ More than just a competitor’s fear of losing the tactical fight, technological superiority has the potential to make it too financially costly to fight in the first place; though as in the Cold War this could be a decades-long endeavor. It was a stated goal of the 2006 QDR to minimize costs to the U.S. while imposing costs on adversaries,²¹ but as Director of National Intelligence Mike McConnell shows, this goal is not easily realized. “European colleagues ... are able to build, launch, and operate a new satellite system in about five years and for less than a billion dollars. By contrast, a U.S. spy satellite

²⁰ DOD, *Quadrennial Defense Review Report*, 18.

²¹ *Ibid.*, 2-3.

system, although admittedly more complex than a European equivalent, can take more than ten years and cost billions of dollars to develop.”²²

The second Rumsfeld S&R priority, decision superiority, is the corollary to information dominance discussed in Appendix B. According to the 2004 National Military Strategy, decision superiority is the ability to make decisions better and faster than an adversary. “The joint force will use superior intelligence and the power of information technologies to increase decision superiority, precision and lethality of the force.”²³ With respect to S&R, it “requires new ways of thinking about acquiring ... information. It necessitates new ideas for ... [ISR] assets that provide knowledge of adversaries. Decision superiority requires precise information of enemy and friendly dispositions, capabilities, and activities, as well as other [relevant] data.”²⁴

Akin to Colonel John Boyd’s “OODA-loop”²⁵ decision cycle, military practitioners constantly strive to think and act faster than their opponents. However, as evidenced in both the Afghanistan and Iraq wars, as well as the ongoing global war against radical Islamists, the information dominance precursor is not achievable.²⁶ Thus,

²² Mike McConnell, "Overhauling Intelligence," 57-58.

²³ DOD, *The National Military Strategy*, 16.

²⁴ *Ibid.*, 19.

²⁵ Observe, Orient, Decide, Act. For more information see http://www.powerseductionandwar.com/archives/ooda_and_you.phtml.

²⁶ See Appendix B for a more detailed discussion of information dominance.

by extension, the U.S. does not have the ability to achieve decision superiority on the scale predicted by Rumsfeld's vision.

The intent to gain and maintain decision superiority is tied to and supported by the third priority category, persistent surveillance, arguably the most discussed component of the Rumsfeld S&R vision. Written in 2004, Joint Publication (JP) 2-01 states that:

Long dwell ISR platforms such as the Global Hawk and Predator UAVs [unmanned aerial vehicles], distributed undersea and unattended ground sensors, battlefield surveillance radars, and special operations forces (SOF) have enabled a paradigm shift in which it is possible to provide near-continuous surveillance over large portions of the battlespace to monitor, track, characterize and report on moving objects and dynamic events.²⁷

In providing guidance for full-spectrum intelligence collection strategies, JP 2-01 emphasizes the need for “near-continuous, all weather, day/night surveillance of the battlespace ... facilitated by the effective integration and synchronization of all theater and national ISR assets and resources ... in a persistent surveillance, as opposed to periodic reconnaissance, mode.”²⁸ JP 2-01 maintains that persistent surveillance provides for the effective use of precision-guided munitions and is integral in defeating an adversary's deception and denial efforts.²⁹

²⁷ DOD, *Joint Publication 2-01, Joint and National Intelligence Support to Military Operations* (Washington, D.C., 2004), III-24.

²⁸ Ibid.

²⁹ Ibid.

In order to fill this need, the 2006 QDR increased twofold the procurement of UAVs, particularly the Predator and Global Hawk systems.³⁰ The 2006 QDR advocated further for “systems that can penetrate and loiter in denied or contested areas”³¹ in order to strategically shape nation-state choices and prevent non-state actors from gaining or using weapons of mass destruction. However, this persistence is predicated on assumed levels of access to contested or denied areas which cannot be guaranteed.

Other than limited SOF and the limited covert capabilities of other U.S. government agencies, ground-based S&R forces do not operate within contested or denied areas without being overtly deployed under conflict conditions. Thus proponents of the Rumsfeld persistent surveillance initiatives champion the universality of air/space-based S&R assets during both peacetime and combat. However, because persistent surveillance “requires collection systems and assured access to air, land, sea and space-based sensors,”³² opponents of the Rumsfeld initiatives challenge the base assumption that these systems will function as advertised in truly contested areas. Persistent surveillance has not been tested against an adversary that is wholly fighting to counter U.S. capabilities. Therefore, just like the un-supported arguments surrounding information dominance, assured access remains a questionable precondition for such S&R capabilities.

³⁰ DOD, *Quadrennial Defense Review Report*, 46.

³¹ *Ibid.*, 31, 35.

³² DOD, *The National Military Strategy*, 19.

There are other points of conflict within the persistent surveillance discussion, but few are as contentious as the above. Namely, that mission requirements usually exceed platform capabilities and availability, often requiring high-demand, low-density assets that are not resident with the theater of operations.³³ This concern can be countered by the global reach and increased production of many systems. Another issue is the need for employing “secure broadband communications into denied or contested areas to support penetrating surveillance and strike systems.”³⁴ A possible counter for this concern is that whatever infrastructure backbone is supporting the surveillance system can also support the requisite communication needs. The fourth and last notable concern is the level of reliance on space-based assets needed to support persistent surveillance.

The 2006 QDR tasked the DOD intelligence community, in cooperation with the Director of National Intelligence, to implement an imagery intelligence approach designed to achieve “persistent collection capabilities.”³⁵ Along with some aerial based improvements in moving target indicators and synthetic aperture radar, the core assets were to be space-based. The QDR maintained that “the Space Radar program (in development) will provide persistent, all-weather, day and night surveillance and reconnaissance ... [with the] capability to identify and track moving ground targets in

³³ DOD, *Joint Publication 2-01*, III-10, 24.

³⁴ DOD, *Quadrennial Defense Review Report*, 31.

³⁵ *Ibid.*, 57.

denied areas.”³⁶ It also assessed that the U.S. would retain its advantage across all space-based capabilities by staying at least one technology generation ahead of both foreign and commercial competitors.³⁷ Space-enabled operations were the lynchpin needed to realize the Rumsfeld S&R vision, and today’s space capability far exceeds what was envisioned at the time. In fact, space enabled operations have progressed so much that both civilian and military activities are now dependent on them.

Everett Doman, Associate Professor of Comparative Military Studies at the U.S. Air Force’s School of Advanced Air and Space Studies, observes that the U.S. has become so reliant on space-based systems that it is now vulnerable to significant new challenges if it fails to maintain them.³⁸

No nation relies on space more than the United States – none is even close – and its reliance grows daily. A wide spread loss of space capabilities would prove disastrous for American military security and civilian welfare. America’s economy would collapse, bringing the rest of the world down with it. Its military would be obliged to hunker down in a defensive crouch while it prepared to withdraw from dozens of then-untenable foreign deployments.³⁹

With the extensive proliferation of technologies in today’s competitive and interconnected society, U.S. dominance in the global common of space should not be accepted as a foregone conclusion.

³⁶ Ibid.

³⁷ Ibid., 55.

³⁸ Everett C. Dolman, "A Debate About Weapons in Space," 165.

³⁹ Ibid., 163.

With this in mind, the 2008 Joint Operating Environment (JOE) provides the Joint Force with two-pronged guidance: “defend the spaced-based systems on which so many of its capabilities depend, [and] anticipate the inevitable attack and know how to operate effectively when these attacks degrade those systems.”⁴⁰ Despite warnings like this one, S&R organizational trends continue to rely on space-based systems for their success, often as the single point of failure. An exploration of threat capabilities in the next chapter will show the vulnerability such reliance would forecast.

At first glance, the fifth Rumsfeld S&R category, increase SOF, may seem to contradict the thesis premise that the U.S. is overly dependent on air/space-based collection assets; after all, the 2006 QDR said that since 2001 SOF experienced an 81% increase in baseline budget, and a key 2007 programmatic decision increased SOF manning by a further 15%.⁴¹ The Army would add one-third more Special Forces battalions, the Navy would increase SEAL (Sea Air Land) team manning and the Air Force would create an UAV Squadron under U.S. Special Operations Command.⁴² While this section is not intended to dwell on the pros and cons of using SOF for operational S&R, it is undeniable that in many circumstances these forces provide a useful balance to the air/space systems – under many, but not all circumstances. When the 2004 National

⁴⁰ United States Joint Forces Command, *The Joint Operating Environment: Challenges and Implications for the Future Joint Force*, (Suffolk, VA, 2008), 23.

⁴¹ DOD, *Quadrennial Defense Review Report*, 5-6, 44.

⁴² Ibid.

Military Strategy (NMS) noted that “human collectors are a critical element in the collection system,”⁴³ it was speaking of far more than just SOF. After all, there are only a few situations where the Combatant Commander (CCDR) can rely solely on SOF as his main ground-based S&R force.

By way of review, Secretary Rumsfeld tasked DOD to “improve effectiveness dramatically across civilian and military functions as the foundation for increased efficiency.”⁴⁴ It was this goal of technological balance and efficiency that guided the departments’ S&R transformation. This resulted in a number of technology leaps that dramatically increased the effectiveness of CCDR S&R, primarily aerial and space-based systems. Ironically, Secretary Rumsfeld’s reliance on concepts such as RMA, NCW, the universal substitution of information for mass, and the belief in decision superiority may have limited DOD’s S&R capabilities more than it helped. In the words of military historian Martin Van Creveld:

Whichever way one looks at it, the conclusion is always the same. The conduct of war against an intelligent opponent differs from the management of a large-scale technological system precisely in that efficiency and effectiveness ... are not the same even in the short run, or (one might well argue) particularly in the short run. On the contrary, there are any number of occasions when military effectiveness is not

⁴³ DOD, *The National Military Strategy*, 19.

⁴⁴ DOD, *Quadrennial Defense Review Report*, 65.

only compatible with diminished efficiency but positively demands that it be sacrificed.⁴⁵

As will be evident in the next section, DOD leadership since the Rumsfeld era incorporated this concern into a number of talking points, but made little change to the constructs imposed on the S&R community.

Current S&R Priorities

While there are promising signs that senior leaders are aware of the potential pitfalls discussed in the previous sections, this awareness has yet to translate into acquisition guidance that corrects for the negative trends. According to Del Kostka, a Technical Executive with the National Geospatial-Intelligence Agency, “the complex acquisition process through which DOD identifies, procures, and implements advanced ISR systems is characterized by gaps in capabilities, growing competition for assets, and systems that do not fully complement one another.”⁴⁶ He states that this is in large part due to DOD’s lack of a comprehensive joint process to define and validate ISR requirements and obtain systems that support warfighting needs. “The significance of this shortfall is immense. Without a unified investment management approach, each independent service has aggressively pursued independent ISR capabilities that are

⁴⁵ Martin L. Van Creveld, *Technology and War: From 2000 B.C. to the Present* (New York: The Free Press, 1991), 318.

⁴⁶ Del C. Kostka, "Moving Toward a Joint Acquisition Process to Support ISR," *Joint Forces Quarterly*, no. 55 (4th Quarter 2009): 70.

tailored to their own unique missions.”⁴⁷ Though not a new issue in military acquisition, this is indicative of the fact that services were not satisfied that S&R acquisition trends were meeting their needs. This would not be an issue if the department operated without resource constraints, but in a zero-sum gain environment such conflicts garner a lot of attention.

Concerned with the lack of cohesion, the 2004 National Defense Authorization Act (NDAA) directed DOD to “develop a comprehensive ‘roadmap’ to guide development and integration of DOD ISR capabilities for fiscal years 2004 through 2018.”⁴⁸ The NDAA also required DOD to create an ISR Integration Council to address ISR integration and coordination issues with the Director of National Intelligence (DNI).⁴⁹ Though it is more likely that they were concerned with budget rather than capability issues, Congress recognized that DOD was struggling for a comprehensive S&R development and acquisition plan, and this struggle was starting to affect other members of the U.S. intelligence community.

In accordance with the NDAA’s direction, DOD developed its ISR Roadmap. As input to the process, DNI Mike McConnell aptly stated that “The U.S. intelligence community ... needs to know where collection gaps exist, where it needs greater specific

⁴⁷ Ibid., 70.

⁴⁸ Ibid., 72.

⁴⁹ Ibid.

intelligence, and on what areas it is overly focused.”⁵⁰ However, according to a 2007 Government Accounting Office (GAO) assessment, all the roadmap provided was a catalogue of current ISR capabilities. It did not identify funding priorities, measure acquisition progress, or most importantly, identify future requirements needs. “Also, the Roadmap does not yet clarify what ISR requirements are already filled or possibly saturated, identify critical gaps for future focus, or define requirements for meeting the goal of global persistent surveillance.”⁵¹

With this lack of specificity in mind, the 2008 National Defense Strategy (NDS) established three priorities that dramatically deviate from previous defense policy and may eventually translate into systems acquisitions. These priorities include: hedging against loss of advantages, the need for redundancy, and the ability to function after an enemy attack.⁵²

As to the first priority, the 2008 NDS speaks extensively about reducing risks and shaping global trends through the development of equipment and capabilities, dissuasion, and deterrence. “The Department should also develop the military capability and capacity

⁵⁰ Mike McConnell, "Overhauling Intelligence," 55.

⁵¹ United States Government Accountability Office, "Intelligence, Surveillance, and Reconnaissance: Preliminary Observations on DOD's Approach to Managing Requirements for New Systems, Existing Assets, and Systems Development," Testimony before the Subcommittee on Air and Land Forces, Committee on Armed Services, House of Representatives, (Washington, D.C.: USGAO 2007), introduction.

⁵² DOD, *The National Defense Strategy*, (2008), 5.

to hedge against uncertainty.”⁵³ Acknowledging the fact that U.S. forces may have to operate without a complete understanding of the operational area is a healthy dose of realism which contrasts with earlier ideals. One prime way the department plans to hedge against this future uncertainty is the development of redundant systems, the second NDS S&R priority.

“The Department will invest in hedging against the loss or disruption of our traditional advantages, not only through developing mitigation strategies, but also by developing alternative or parallel means to the same end.”⁵⁴ The NDS is quick to point out that this does not mean the U.S. will simply have more of a given capability, but rather will seek to achieve similar effects through system redundancy. As the next chapter will show, achieving effective redundancy in S&R systems will require an increased reliance on ground-based capabilities.

After acknowledging that the U.S. will not operate with perfect knowledge, the next logical step is to preserve the ability to function after first contact; the third NDS priority. “We must build both our ability to withstand attack ... and improve our resiliency beyond an attack. An important change in planning for the myriad of future potential threats must be post-attack recovery and operational capacity.”⁵⁵ Significant change is required if the current S&R apparatus is to function effectively during and after

⁵³ Ibid.

⁵⁴ Ibid., 22.

⁵⁵ Ibid., 12.

a concerted attack, particularly with the proliferation of denial technologies and weapons of mass destruction (WMD). “Should the worst happen, and we are attacked, we must be able to sustain operations during that attack and help mitigate the consequences of WMD attacks at home or overseas.”⁵⁶

Despite the clear and reasonable priorities expressed in the 2008 NDS, the GAO assessed in a follow-on report that DOD still lacked a defined vision to guide ISR investments. “Without a clear vision of the desired ISR end state and sufficient detail on existing and planned systems, DOD decision makers lack a basis for determining where additional capabilities are required, prioritizing investments ... as well as identifying areas where further investment may not be warranted.”⁵⁷ In short, despite some new focus in the 2008 NDS and lively discussion among the department’s senior leadership, DOD has not indentified “critical gaps for future focus.”⁵⁸ As such, S&R resource allocation paradigms established by Secretary Rumsfeld remain essentially intact.

In summary, this section described the evolution and immediate effects of DOD S&R priorities from the 1950s through today. The department established decision superiority and persistent surveillance as the metrics of success and directed the

⁵⁶ Ibid., 15.

⁵⁷ United States Government Accountability Office, Intelligence, Surveillance, and Reconnaissance: DOD Can Better Assess and Integrate ISR Capabilities and Oversee Development of Future ISR Requirements, Report to the Subcommittee on Air and Land Forces, Committee on Armed Services, House of Representatives, (Washington, D.C.: USGAO 2008), introduction.

⁵⁸ Ibid.

acquisition of a force structure dependent on technological air and space-based solutions.

At the height of perceived U.S. information superiority, note what U.S. Army General David Petraeus, then commander of Multi-National Forces Iraq, said in his guidance to subordinate commanders in 2007:

We are in a fight for intelligence – all the time. Intelligence is not a ‘product’ given to a commander by higher headquarters, but rather something we gather ourselves, through our own operations. Tactical reporting, from civilian and military agencies, is essential: there are thousands of eyes out in your area – all must act as scouts, know what to look for, and be trained and ready to report it ... Most actionable intelligence will come from locally produced [human intelligence], tactical reporting, follow-up of [improvised explosive devices] and sniper attacks, detainee interrogations, and [signals intelligence]. Work with what you have.⁵⁹

Though some senior leaders may recognize the challenges with the current S&R construct, the U.S. has not made a concerted effort to address them.

Projected S&R Capabilities

The remainder of this chapter describes the systems that will be available to the operational commander in the foreseeable future. The section focuses primarily on known capabilities; however, applicable trend analysis often provides insights into anticipated future capabilities. Realizing the scope and scale of the assets within the S&R

⁵⁹ David H. Petraeus, *Multinational Force-Iraq Counterinsurgency Guidance*, 6 June 2007; available from http://www.airforce.forces.gc.ca/CFAWC/Contemporary_Studies/2007/2007-Jun/2007-06-06_MNF-I_COIN_Guidance-Summer_2007_v7_e.asp; Internet; accessed October 6, 2009.

community, well over \$47 billion in 2008,⁶⁰ some systems will represent a more expansive family of systems. Obviously system security classification limits the fidelity of publishable asset capabilities, but not so much so that it is detrimental to this analysis.⁶¹ Commanders can apply a large degree of creativity in their intelligence collection planning, often using non-standard collection systems and techniques as well as pairing or sequencing a series of assets to meet the objective. This substitution of nickels for dollars is accounted for in the next chapter's asset comparison, and predicts potentially serious sub-optimal outcomes through such creative substitution.

Air/Space Capabilities

In their article, "Global Distributed ISR Operations: The Changing Face of Warfare," U.S. Air Force (USAF) Lieutenant General David Deptula and Colonel James Marrs make the case for a global network-centric warfighting capability. "This rapidly evolving paradigm, called distributed ISR operations, links platforms and sensors, forces forward, and human ISR warfighting expertise around the globe in ways that make networked combat operations routine."⁶² The Air Force linked a series of communication assets and space systems to build "an architecture that allowed U-2, Global Hawk, Predator, and Reaper aircraft to transmit regionally collected data to exploitation

⁶⁰ Del C. Kostka, "Moving Toward a Joint Acquisition Process to Support ISR," 72.

⁶¹ Security classification also limits useful discussion of CCDR's Integrated Priority List (IPL), Joint Urgent Operational Needs Statement (JUONS), and Request for Forces (RFF) documents.

⁶² David A. Deptula and James R Marrs, "Global Distributed ISR Operations: The Changing Face of Warfare," *Joint Forces Quarterly*, no. 54 (3rd Quarter 2009): 110.

locations around the globe.”⁶³ This architecture evolved into the AN/GSQ-272 Sentinel weapons system, also known as the Distributed Common Ground System (DCGS). DCGS currently links twenty global locations with nine more sites scheduled for future development.⁶⁴

While the Air Force calls DCGS a “weapon system,” in actuality it is a satellite-supported command, control, and analysis network that manages all U2, Global Hawk, Reaper, and Predator systems; the litany of reasons why the aircraft and the pilot should be on separate continents is not important here. In that each DCGS site can assume the duties of any other site, and is capable of controlling any supported system around the globe, national leaders have a single point of contact to reallocate systems as needed; what the authors call “global ISR flexibility.”⁶⁵ Thus the Sentinel architecture and accompanying USAF ISR groups are “the foundation for a new operational paradigm that executes regionally focused, globally networked joint and allied ISR operations.”⁶⁶

As one might expect, not everyone agrees with the DCGS concept of centralized control of ISR assets. While Colonel Howcroft notes that technological advances provide current commanders with unparalleled abilities to monitor and collect intelligence, the question of what technology the U.S. should buy has not been completely answered.

⁶³ Ibid.

⁶⁴ U.S. Air Force, *Factsheets*, available from <http://www.af.mil/information/factsheets/>; Internet; accessed 9 February 2010: Air Force Distributed Common Ground System.

⁶⁵ David A. Deptula and James R Marrs, "Global Distributed ISR Operations," 114.

⁶⁶ Ibid., 112.

“Based on the wars we will probably fight and our contemporary doctrine, it seems clear that there is a need to develop a number of smaller, decentralized collection systems rather than depend on a few, more capable systems managed and directed by a distant centralized hierarchy.”⁶⁷ In discussing operations in Iraq, U.S. Army General Ray Odierno, Commander of Multi-National Forces-Iraq, said that the operational environment demonstrated that ISR assets should reside at the lowest echelon possible, and should not be centrally controlled at the national level.⁶⁸ Echoing the concerns of many ground commanders, General Odierno stated further that “in today’s environment, a commander must plan operations based on specific ISR systems available, and they are often the sole determining factor in what the unit can or cannot do operationally.”⁶⁹ This concern obviously relates to both ground and air/space-based systems. Due to requisition complexities, number of assets available, asset reallocation, on-station time, etc., concerns remain over the ability of either the current or predicted structure of aerial ISR to fully support the needs of the ground commander.

With the DCGS command and control structure in mind, this section will now assess the capabilities of the three main components of air/spaced based ISR: unmanned aerial systems (UAS), manned aircraft, and satellites. Either by design or operator

⁶⁷ James R. Howcroft, "Technology, Intelligence, and Trust," 26.

⁶⁸ Raymond T. Odierno, Nichol E. Brooks, and Francesco P. Mastracchio, "ISR Evolution in the Iraqi Theater," *Joint Forces Quarterly*, no. 50 (3rd Quarter 2008): 52.

⁶⁹ *Ibid.*, 53.

creativity, many of the below systems perform duties in addition to S&R. Furthermore, while it is also understood that any system in the inventory has the potential to support the commander's S&R effort, assets with minimal impact are not included in this list. The reader should note that volumes of data exist for each of the discussed systems, but only data critical to the crux of this analysis is included. Thus information such as optic/radar physical pan limitations, while exploitable by a knowledgeable enemy force and required for a holistic discussion of system capabilities, are generally outside the scope of this paper.

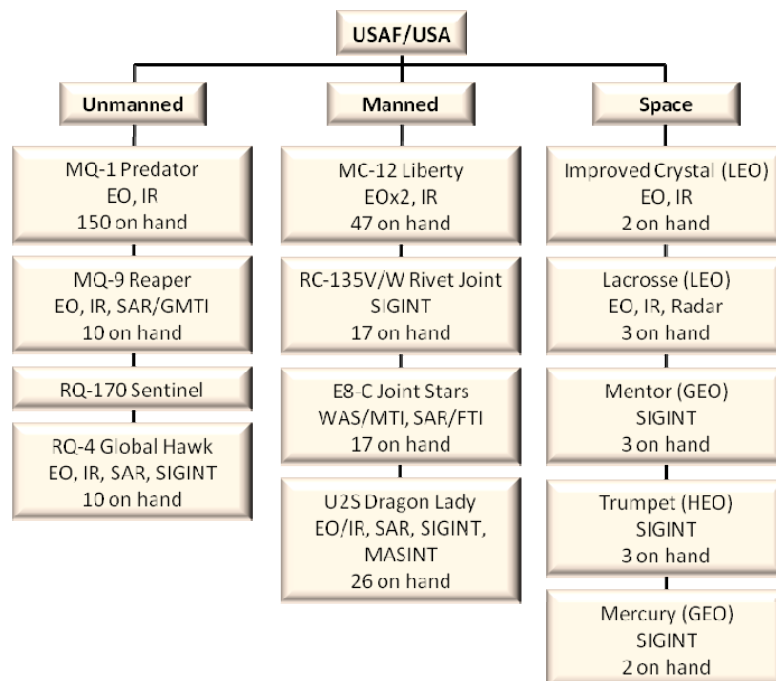


Figure 3: USAF and USA Aerial/Space-Based S&R Assets⁷⁰

⁷⁰ See Appendix C for specific system characteristics and source data.

UAS's are represented by the MQ-1 Predator,⁷¹ the MQ-9 Reaper, the RQ-170 Sentinel, and the RQ-4 Global Hawk. The MQ-1 Predator's primary mission is interdiction and armed reconnaissance against critical, perishable targets; it has the ability to self-designate and launch two AGM-114 Hellfire missiles. "When the MQ-1 is not actively pursuing its primary mission, it acts as the Joint Force Air Component Commander [JFACC]-owned theater asset for reconnaissance, surveillance and target acquisition in support of the Joint Forces commander [JFC]."⁷² The MQ-1 carries an Electro-optical (EO) (daylight) TV camera, an Infra-red (IR) (thermal) camera, as well as a laser illuminator/range finder.⁷³

Similar to the MQ-1, the MQ-9 Reaper is primarily a strike asset for emerging targets, but it can also fulfill a theater S&R role.⁷⁴ The Reaper is an overall increased capability version of the Predator; "flying twice as high, twice as fast, and carrying four times the weapons."⁷⁵ In addition to its EO/IR cameras, the MQ-9 also carries a Synthetic Aperture Radar (SAR) and Ground Moving Target Indicator (GMTI). SAR is a system

⁷¹ Discussions on the MQ-1 also account for the U.S. Army's MQ-1C Sky Warrior (or Warrior) program.

⁷² U.S. Air Force, *Factsheets*, MQ-1 Predator.

⁷³ Ibid.

⁷⁴ U.S. Air Force, *Factsheets*, MQ-9 Reaper.

⁷⁵ GlobalSecurity.org, *Military, Systems, Aircraft*, 14 December 2009, available from <http://www.globalsecurity.org/military/systems/aircraft/index.html>; Internet; accessed 13 February 2010: UAV/MQ-9B Reaper.

that uses radar waves to create imagery through most cloud and dust obscurants, and the GMTI uses radar to identify and/or track moving ground vehicles.⁷⁶

The RQ-170 Sentinel, not to be confused with the DCGS system by the same name, remains a classified system, but is included in this list as an example of the potential changes in the future of unmanned S&R systems. The Air Force acknowledges that it is a low observable UAS under development to support the ISR needs of the CCDR.⁷⁷ International media outlets covering Operation Enduring Freedom describe the system as a stealth-enabled jet-powered UAV.⁷⁸ The Sentinel's performance characteristics demonstrate substantial progress in UAS development and are but a glimpse of what designers envision for the future.

The final system in this category is the RQ-4 Global Hawk, "a high-altitude, long-endurance unmanned aircraft system with an integrated sensor suite" that provides global ISR support and will eventually replace the USAF U-2 airplane.⁷⁹ The Global Hawk is different from the remainder of this list in a number of ways. It is unarmed and thus does not have a strike mission; it only creates still images versus full-motion video; and it is

⁷⁶ Ibid.

⁷⁷ U.S. Air Force, *Factsheets*, RQ-170 Sentinel.

⁷⁸ Jane's, *Unmanned Aerial Vehicles and Targets*, 10 February 2010, available from http://juav.janes.com/docs/juav/browse_section.html; Internet; accessed 13 February 2010: Unmanned Aerial Vehicles/Lockheed Martin RQ-170 Sentinel.

⁷⁹ U.S. Air Force, *Factsheets*, RQ-4 Global Hawk.

designed with the potential to carry a Signals Intelligence (SIGINT) package in lieu of its SAR and EO/IR sensors.

Countries around the globe remain as focused as the U.S. on exploiting UAS technology. In many instances this includes U.S.-based companies legally selling technology to foreign entities; aside from the RQ-170 Sentinel, each of the above systems has been sold to international customers. Given this, the U.S. cannot assume that potential adversaries are ignorant of its possible UAS capability.

The U.S.'s manned aircraft capabilities are represented by the USAF MC-12 Liberty, RC-135V/W Rivet Joint, E-8C Joint Stars, and U2S Dragon Lady. The USAF MC-12W Liberty is a medium- to low-altitude, twin-engine turboprop aircraft with a primary mission to provide ISR support directly to ground forces. The MC-12W is a JFACC asset in support of the JFC.⁸⁰ The system produces full motion video using one of two daylight cameras or an IR camera. The aircraft has a missile warning system with limited countermeasure dispensing capabilities. The system has been sold to Iraqi and British forces and is basically the same as the U.S. Army's Medium Altitude Reconnaissance and Surveillance System (MARSS).⁸¹

The RC-135V/W Rivet Joint reconnaissance aircraft supports theater and national level consumers with a sensor suite that detects, identifies and geolocates signals

⁸⁰ U.S. Air Force, *Factsheets*, MC-12.

⁸¹ GlobalSecurity.org, *Military, Systems, Aircraft*, RC-12/MC-12 Liberty.

throughout the electromagnetic spectrum.⁸² The communications intelligence (COMINT) and electronic intelligence (ELINT) sensor suites have progressively upgraded on approximately 18 month intervals over the life of the fleet.⁸³

The E-8C Joint Surveillance Target Attack Radar System's (J-STARS) primary mission is to provide theater air and ground commanders with ground surveillance to support attack operations.⁸⁴ Using a side-looking phased-array radar, the system can operate in two modes: Wide Area Surveillance/Moving Target Indicator (WAS/MTI) and Synthetic Aperture Radar/Fixed Target Indicator (SAR/FTI). The system has some limited capability to detect helicopters and slow moving fixed wing aircraft,⁸⁵ and carries an unspecified threat-sensing and chaff dispensing capability.⁸⁶

The U2S Dragon Lady high-altitude/near space reconnaissance and surveillance aircraft provides IMINT (EO/IR/SAR), SIGINT, and electronic measurements and signature intelligence (MASINT) in direct support of U.S. and allied forces. The

⁸² U.S. Air Force, *Factsheets*, RC-135V/W RIVET JOINT.

⁸³ GlobalSecurity.org, *Military, Systems, Aircraft*, RC-135.

⁸⁴ U.S. Air Force, *Factsheets*, E-8C JOINT STARS.

⁸⁵ Ibid.

⁸⁶ Jane's, *All the World's Aircraft*, 10 February 2010, available from http://jawa.janes.com/docs/jawa/browse_section_results.jsp?SelPub=jawa&bucket=Section&selected=AIRCRAFT+-+FIXED-WING+-+MILITARY&sort=Country-false&pageCount=-1; Internet; accessed 16 February 2010: Northrop Grumman E-8 Joint Stars.

MASINT capability provides indications of recent activity in a particular area.⁸⁷ The aircraft is equipped with a surface to air missile launch and tracking/jamming system.⁸⁸

While any craft is capable of carrying a sensor, these four systems represent the full scope of available manned ISR systems. Though the modern battlefield is full of rotary-wing aircraft, they typically only assist in answering operational level commander's critical information requirements (CCIR) through the indirect results of their tactical responsibilities. In that they are typically in a supporting role, the S&R outputs of rotary-wing systems are incorporated into the ground capabilities described in the next section.

The last segment of this aerial ISR section is space-based systems. Though these systems exist primarily to support national and strategic objectives or provide commercial imagery, they routinely support the information needs of the operational commander. Assessing how supportive they can be, however, requires some conjecture based on existing technologies. For even though an amateur telescope can track most space-based systems, and the launches, flight paths, and schedules of space assets are readily accessible through multiple open-source intelligence venues,⁸⁹ the full capabilities of each given system remain classified.

⁸⁷ U.S. Air Force, *Factsheets*, U-2S/TU-2S.

⁸⁸ Jane's, *All the World's Aircraft*, Lockheed Martin U-2S.

⁸⁹ Jane's, *Space Systems and Industry*, 10 February 2010, available from http://jsd.janes.com/docs/jsd/browse_section_results.jsp?SelPub=jsd&bucket=Section&selected=SPACEC

“In all, more than 800 satellites are used for military and commercial purposes according to an estimate made in 2005. Nearly half of these are operated by the U.S. Government or private sector.”⁹⁰ This includes such well known constellations as the Global Positioning System and Milstar communications system,⁹¹ as well as meteorological, ballistic/nuclear launch tracking,⁹² and surveillance programs designed specifically to detect and track objects in space.⁹³ Among these, those systems designed to provide IMINT or SIGINT are of particular value to the operational commander, despite the fact that they comprise a small fraction of total space-based assets. While the U.S. is currently experiencing a potential gap in space-based intelligence due to political and budget conflicts,⁹⁴ the below listed systems represent both current and anticipated

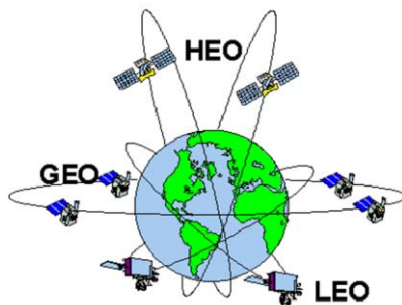


Figure 4: Satellite Orbits

capabilities.

IMINT satellites use film, electronic cameras and/or radars to produce images of objects on the ground; some are capable of better than 4 inch resolution. Operating in low earth orbit (LEO), (see

RAFT++DEFENCE&sort=Country=false&pageCount=-1; Internet; accessed March 1, 2010: Lacrosse/Onyx series.

⁹⁰ T.W. Lee, *Military Technologies of the World*, (Westport, CT: Praeger Security International, 2009), 218.

⁹¹ U.S. Air Force, *Factsheets*.

⁹² Jane's, *Space Systems and Industry*, SBIRS.

⁹³ Ibid., SBSS (Space-Based Space Surveillance).

⁹⁴ GlobalSecurity.org, *Space Menu, Systems*, 14 December 2009, available from <http://www.globalsecurity.org/space/systems/index.html>; Internet; accessed 28 February 2010: Imagery Intelligence/Lacrosse/Onyx.

Figure 4),⁹⁵ a resolution of several meters is useful in identifying vehicles and installations while resolutions around ten meters can locate facilities such as airfields and ports.⁹⁶ The two IMINT constellations used by the U.S. are the Improved Crystal optical system and the Lacrosse imaging radar.

The Improved Crystal satellite is also known as Advanced Crystal, IKON, and KH-12.⁹⁷ It is a LEO system that is basically a Hubble Space Telescope with a rocket engine for minor maneuvers. Its sensors operate in visible light, near IR, and thermal IR. Despite its technological superiority over other photographic intelligence systems, the Improved Crystal is still unable to ‘see’ through clouds.⁹⁸ While this poses a problem for intelligence collection, controllers can either direct the coverage to cloud-free areas or simply wait for later satellite passes. “While this procedure may have been adequate for peace-time operations, it is clearly inadequate for war-time target acquisition.”⁹⁹

⁹⁵ GlobalSecurity.org, *Space Menu, Systems*, SBIR; National Aeronautics and Space Administration, Global Change Master Directory, *Ancillary Description Writer's Guide*, 2008, <http://gcmd.nasa.gov/User/suppguide/platforms/orbit.html> (accessed February 4, 2010). Low Earth Orbits (LEO) are between 80 km and 2000 km. Geosynchronous Orbits (GEO) have a revolution of exactly one day at an altitude of 35,786 km; the satellite continually looks at the same spot on the earth. High Earth Orbits/Highly Elliptical Orbits (HEO) have a low perigee (about 1000 km) and a high apogee over 35,786 km.

⁹⁶ Ibid., Imagery Intelligence/Overview.

⁹⁷ Jane's, *Space Systems and Industry*, Improved Crystal.

⁹⁸ GlobalSecurity.org, *Space Menu, Systems*, Imagery Intelligence/Lacrosse/Onyx.

⁹⁹ Ibid.

The Lacrosse radar imaging spacecraft, also known as Vega and Onyx, carries an unspecified infra-red capability and a phased array radar.¹⁰⁰ It is essentially a smaller version of the Improved Crystal satellite.

Though proven and highly capable, the continued availability of space-based imagery is subject to the ever-changing political desires of U.S. leadership. In 2009, the U.S. Congress decided not to fund an FY08 DOD initiative called the Broad Area Space-based Imagery Collector (BASIC). The program called for the purchase of one imaging satellite with commercial-grade optics (approximately 3.6 foot resolution) with the option of a second purchase. The additional constellation was to launch in 2012 in order to avoid a lapse in capability due to the age and fuel remaining in the Improved Crystal spacecraft.¹⁰¹

Later that same year the office of the President authorized the purchase of two additional satellites with equal or better resolution than Improved Crystal.¹⁰² In that it takes from five to seven years to develop and deploy a new spacecraft, the U.S. allocated \$1.7 billion to purchase an increased volume of commercially developed imagery while it attempted to sort through the way ahead for additional systems.¹⁰³

¹⁰⁰ Ibid.

¹⁰¹ Jane's, *Space Systems and Industry*, Improved Crystal.

¹⁰² Ibid.

¹⁰³ GlobalSecurity.org, *Space Menu, Systems*, Imagery Intelligence/FIA - Future Imagery Architecture to BASIC.

This specific discussion highlights an operational limitation of all space-based systems; maneuverability. With an obvious need to extend the lives of the spacecraft, U.S. leadership must weigh the need to reposition an asset from its existing orbit against its resulting shortened lifespan; when it runs out of fuel the system is lost. Even with all of the international and domestic attention focused on Operation Enduring Freedom in Afghanistan in 2010, U.S. leadership said it would take up to two years to reposition three GPS satellites to support troops that were losing coverage in the mountainous terrain.¹⁰⁴ Should the operational commander find himself operating outside of the predicted conflict area that defined a spacecraft's original orbit location, he must be prepared to conduct the operation with limited up-to-date satellite imagery capability.

The U.S. SIGINT satellite system currently consists of three constellations in both geostationary and highly elliptical orbits. The systems are designed to assist in missile launch tracking as well as detect transmissions from radios, radars, and other such electronic systems. This data is useful in locating, typing, and possibly tracking adversaries systems. The constellations are not capable of intercepting communications over wired land lines such as a standard telephone system and global under-sea fiber optic cables. The overall system is designed to have each constellation complement the

¹⁰⁴ Thom Shanker and Eric Schmitt, More Satellites Will Act as Eyes for Troops, *The New York Times*, 24 February 2010, available from <http://query.nytimes.com/gst/fullpage.html?res=9C07E2DD143CF937A15751C0A9669D8B63&scp=5&sq=thom+shanker&st=nyt>; Internet; accessed 3 March 2010.

other, though all are capable of monitoring the entire electro-magnetic radio spectrum frequency range.¹⁰⁵

For over a decade the U.S. has been planning to merge the two larger and more capable systems, Mentor and Trumpet, into a single system called Intruder, but political and budgetary debates have delayed the DOD plan.¹⁰⁶ These two constellations work in concert with the smaller Mercury system to enable the U.S. to monitor nearly any spot on earth. All three constellations communicate and relay for each other to a number of ground control stations around the world.¹⁰⁷ Operators then use the collected signals data to prioritize tasking more capable systems for further refinement of the potential target location.

The Mentor constellation, also known as Advanced Mentor and Advanced Orion, is in geosynchronous orbit (GEO). This configuration allows each satellite to remain over a single point on the earth and pivot its field of view to observe a desired coverage area. While the exact coverage capability is classified, it is believed capable of monitoring a few thousand miles square at one time. Due to the curvature of the Earth there are gaps in coverage between each satellite. The U.S. attempts to cover these gaps with the smaller Mercury systems and the highly elliptical orbiting (HEO) Trumpet constellation. The

¹⁰⁵ GlobalSecurity.org, *Space Menu, Systems, Signals Intelligence/Overview*.

¹⁰⁶ Jane's, *Space Systems and Industry*, SIGINT.

¹⁰⁷ GlobalSecurity.org, *Space Menu, Systems, Signals Intelligence/Mercury*.

latest satellite in the Mentor constellation was launched in January 2009 and is expected to provide coverage throughout the next decade.¹⁰⁸

The Trumpet constellations' Molniya HEO orbit allows it to cover a particular area of the earth for nearly 8 out of every 12 hours. As the satellite approaches the apex of the orbit, its apogee, the amount of terrain it can monitor increases while signal strength decreases. The last Trumpet satellite was launched in 1997 and it is believed that the constellation maintains apogee coverage over the former Soviet Union.¹⁰⁹

The Mercury constellation, also known as Vortex-II and Advanced Vortex, is a GEO system similar to Mentor but with a smaller field of view.¹¹⁰ Its last launch was in 1994.¹¹¹

Ground Capabilities

From manned, to unmanned, to space-based assets the U.S. maintains a formidable array of aerial S&R capability. It also maintains a world-renowned ground-based combat force. But what of its ground-based S&R capability, and how do the air and ground systems link together to answer the operational commander's information needs? As with the aerial systems, this section will describe the capabilities and limitations of the ground-based S&R force in light of their applicability to the operational commander.

¹⁰⁸ GlobalSecurity.org, *Space Menu, Systems*, Mentor.

¹⁰⁹ Jane's, *Space Systems and Industry*, Trumpet Series.

¹¹⁰ GlobalSecurity.org, *Space Menu, Systems*, Signals Intelligence/Mercury.

¹¹¹ Jane's, *Space Systems and Industry*, SIGINT.

Unlike the aerial systems, most ground-based S&R capability is designed primarily for execution at the tactical, not operational level. Thus, there is little utility in analyzing the capabilities and limitations of each individual system. Rather, applicability to the operational commander is in the aggregate capabilities and limitations of the S&R units he will have available. By analyzing the Global Force Management Implementation Guidance (GFMIG)¹¹² the ground S&R assets available to the CDR fall into two general categories, Special Operations and Ground Maneuver.¹¹³

In conjunction with other national collection agencies, the United States Special Operations Command (USSOCOM) is arguably the primary force provider in support of ground-based operational intelligence collection; especially during pre-conflict operations. The units in Figure 5 highlight all of the assets within USSOCOM that are capable of ground S&R;¹¹⁴ but this does not mean that they are purely S&R focused. While each organization focuses on a given specialty, as a whole, they all train for unconventional warfare, foreign internal defense, special reconnaissance, direct action, combating terrorism, counter proliferation, and information operations.¹¹⁵

¹¹² The GFMIG is a classified document that lists allocated forces available to the CDR for planning contingency operations.

¹¹³ DOD, *Global Force Management Implementation Guidance 2008*, Washington D.C., 2008. The capabilities and limitations of rotary wing aviation assets are incorporated into the parent unit assessments.

¹¹⁴ The chart is not intended to replicate a complete command and control diagram for USSOCOM.

¹¹⁵ United States Special Operations Command Public Affairs, *USSOCOM Fact Book*, 5 March 2010; available from <http://www.socom.mil/SOCOMHome/newspub/pubs/Documents/FactBook.pdf>; Internet; accessed 7 March 2010.

Each U.S. Army Special Forces Group is regionally oriented to support one of the geographic combatant commanders (GCC). This means that when a CCDR factors in rotation and training requirements, he may be able to count on having one battalion within his area of responsibility (AOR) at any given time. In similar fashion, the smaller formations within Naval Special Warfare (NSW) and Marine Special Operations Command (MARSOC) mean that a CCDR may only count on a single SEAL team or MARSOC company within his AOR.

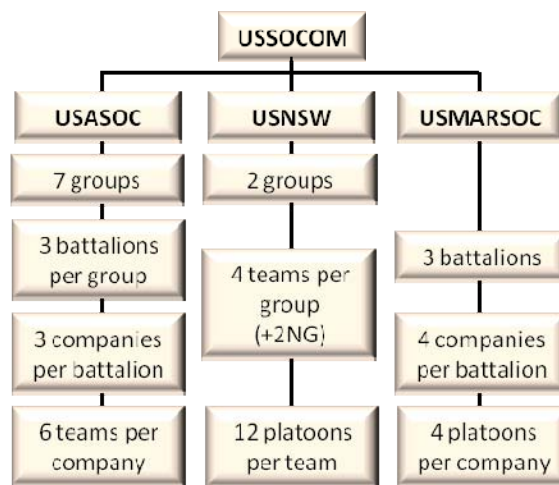


Figure 5: Possible Ground S&R Assets Available to USSOCOM¹¹⁶

The remainder of ground maneuver assets reside within the conventional forces assigned by the Secretary of Defense's "Forces for Unified Command's"

¹¹⁶ United States Special Operations Command Public Affairs, *USSOCOM Fact Book*.

memorandum,¹¹⁷ most of which are managed by the Army and Marine Corps elements within the United States Joint Forces Command (USJFCOM). This section describes their respective capabilities, both designed for S&R and otherwise. As with the SOCOM section, ground support capabilities such as aviation and signals intelligence are incorporated into the overall capabilities of the ground maneuver force.

Regardless of circumstances, the U.S. military will eventually accomplish a given mission. Thus, a brief discussion of specialization is in order. After all, with nearly every ground combat asset supporting Operation Iraqi Freedom since 2004 performing primarily light infantry tasks, why would the U.S. need specialized ground S&R? This is a critical point when discussing current and predicted ground-force structure, because the same Rumsfeld-era transformation goals that fuelled the explosion in aerial ISR have drastically reduced their specialized ground-based partners.

In 1933, Secretary of War Henry Stimson noted in his annual report to the President that “behind the Infantry, Cavalry, and Artillery lies a long history of battle experience out of which have developed certain fundamental methods applying to the tactics, training, and organization of each of these arms and to their combined employment in war.”¹¹⁸ At that time, U.S. armed forces were struggling to adapt to the

¹¹⁷ DOD, *Joint Publication 1, Doctrine for the Armed Forces of the United States* (Washington, D.C., 2009), IV-2.

¹¹⁸ War Department, *Report of the Secretary of War to the President, Annual*, (Washington D.C.: United States Government Printing Office, 1933), 31.

lessons learned from World War I. The advent of armor and aviation led many to believe that historically tested S&R principles were no longer relevant in the face of new technologies. The subsequent 75 years of S&R modifications are the subject of countless analyses, books and monographs focused on this topic. It is sufficient to note, however that since the mid-1990s the U.S. military has seen a steady decrease in specialized ground-S&R capability¹¹⁹ in favor of more general purpose capabilities. However, when tested on a future battlefield, the current and predicted ground combat force may have significant trouble adhering to the time-tested fundamentals of reconnaissance and surveillance.

The overall decrease in S&R capability is felt first and foremost at the nexus of the operational and tactical levels of war. “If a combatant commander determines that the information needed to answer a RFI [request for information] is unavailable, the commander may task organic collection assets or those of a subordinate organization or request multinational or national-level support to satisfy the requirement.”¹²⁰ It is

¹¹⁹ United States Army, *The Official Webpage of the United States Army*, 1 March 2010; available from <http://www.army.mil/info/organization/>; Internet; accessed 9 March 2010. As of 2010, the U.S. Army’s modularity transformation removed all dedicated Corps and Division ground-based S&R forces; the Armored Cavalry Regiment and Divisional Cavalry Squadron respectively. While modularity did create a new Battlefield Surveillance Brigade (BfSB) and added an Armored Cavalry Squadron (ARS) or Reconnaissance/Surveillance/Target Acquisition (RSTA) Squadron to each Brigade, there was still a net-sum capability loss. When one accounts for the Brigade Reconnaissance Troops that were already in each Brigade, the result is a net loss of nine Cavalry Squadrons across the Army – essentially losing three Corps level regiments.

¹²⁰ DOD, *Joint Publication 2-01*, III-21.

common practice within the S&R community for a commander to exhaust the assets at his echelon then task subordinate units to cover remaining information gaps.

A cursory review of the GFMIG reveals that an operational commander's information tasking will move through at least three echelons before a trained organization can be found (see Figure 6 below). By the time a specialized S&R squadron/battalion receives the collection tasking, the corps/MEF (Marine Expeditionary Force), the division, and the brigade/regiment have all added their own information needs to their collection priorities. Even if these squadrons or battalions were solely focused on S&R, which they are not, they are incapable of answering the mass of generated collection needs. Thus commanders must rely on air and space-based systems or operate without the needed information.

The issue of fewer trained S&R forces is exacerbated by the multiple roles they are required to perform. While S&R forces have historically performed both reconnaissance and security missions, they were separate formations providing early warning for the follow-on brigades. Army modularity reduced all but the Stryker Brigade Combat Teams to two combat maneuver battalions, leading brigade commanders to task their reconnaissance squadron to conduct maneuver specific functions within the Brigade

footprint.¹²¹ This means that without timely and accurate aerial and/or SOF information, the first unit to make contact with an enemy force is a maneuver brigade/regiment. This may negate any possible reaction time at the operational level by decisively committing the formation.

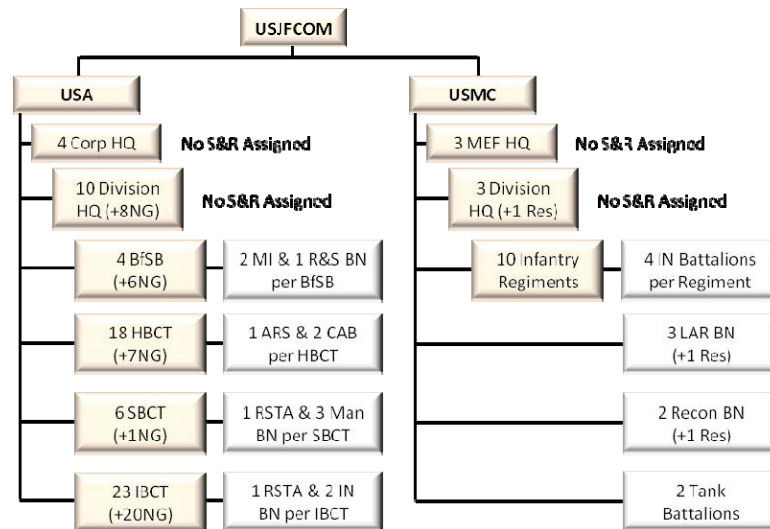


Figure 6: Ground S&R Assets Available to USJFCOM¹²²

In summary, this chapter assessed the capabilities of the entire scope of S&R assets available to the operational commander. From aerial manned and unmanned systems, to space-based sensors, to SOF and ground-maneuver, the U.S. maintains a

¹²¹ The Brigade/Regiment squadron/battalions are specifically designed to operate within and remain supported by the remainder of the Brigade; they are not self-sustaining for any appreciable distance or time.

¹²² USMC Program Assessment and Evaluation Division, *Concepts and Programs*, Washington, D.C.: DMA Marine Corps, 2009, 39-48; United States Army, *The Official Webpage of the United States Army*. NG (National Guard), BfSB (Battlefield Surveillance Brigade), MI (Military Intelligence), HBCT (Heavy Brigade Combat Team), ARS (Armored Reconnaissance Squadron), CAB (Combat Arms Battalion), SBCT (Stryker Brigade Combat Team), IBCT (Infantry Brigade Combat Team), LAR (Light Armored Reconnaissance).

composite S&R capability that is second to none. Should every system work as envisioned the U.S. could reasonably obtain the information dominance it desires; and therein lies the issue. When the limitations of individual systems are comparatively applied to future scenarios, the U.S. may find that it does not have the effective S&R capabilities it currently assumes.

CHAPTER 3

CAPABILITIES GAP ON FUTURE BATTLEFIELDS

By applying DOD's anticipated S&R capabilities against the information needed by the operational commander (see Appendix A for more detail) across the full scope of battlefield considerations, this chapter highlights the information collection gaps that could exist in future conflicts. Beginning with an assessment of the non-permissive aspects of the future operational environment, the chapter describes the current sensor allocation process and then assesses the abilities of S&R assets with respect to terrain, weather, and threat considerations. In so doing, the reader will clearly see the capabilities and limitations of the predicted S&R force.

The Operational Environment

In July of 1949, the United States was confident in its position on the world stage. Though there were innumerable tensions across the globe, the U.S. had the strategic edge – a functioning nuclear weapon; a capability so powerful that defense senior leaders began acquisition and reorganization projects to capitalize on its strength. Pundits and experts wrote scores of books and journal articles on how the U.S. military could use this revolutionary asset to transform the very way wars were fought. However, in August of that same year the Soviet Union successfully tested its own nuclear weapon. It would be an understatement to say that this sent shock waves through the establishment. In a single act, America's primary threat had all but nullified the U.S. decisive advantage.

With a similar belief in its S&R technological superiority and mastery of the global commons of sea, air, space, and cyberspace, could the United States find itself in a similar position today? An understanding of the current and future operational

environment will help to answer this question. In his attempt to do just that, defense policy analyst and Air War College professor Dr. Jeffrey Record said “I believe that the age of large-scale conventional interstate warfare opened by the French Revolution is drawing to a close, and with it the relevance of Clausewitz’s postulation of total war among states.”¹ Dr. Record then goes on to provide a rather substantial list of possible exceptions, including Korea, Taiwan, Syria-Israel, India-Pakistan, or the “emergence of a military peer competitor by the middle of the 21st century.”² Compare this assessment with that postulated in the Joint Operating Environment. “Competition and conflict among conventional powers will continue to be the primary strategic and operational context for the Joint Force over the next 25 years ... a ‘conventional power’ ... is governed by ... recognized norms and codes – conventions.”³ Which one is right? Is the U.S. to prepare for large-scale conventional fights or remain focused on the counter-insurgency activities that typify the current wars? In a word, the answer is both.

In his discussion of the difficulty in establishing national strategy, Dr. Colin Gray,⁴ notes that the future is unforeseeable and nations must make decisions based on historical experience, prudence, and common sense. “We can educate our common sense

¹ Jeffery Record, *The Creeping Irrelevance of U.S. Force Planning*, (Monograph, Carlisle Barracks: Strategic Studies Institute, U.S. Army War College, 1998), 1.

² Ibid., 15.

³ United States Joint Forces Command, *The Joint Operating Environment*, 24.

⁴ Dr. Gray is a Professor of International Politics and Strategic Studies at the University of Reading, England and founder of Washington’s National Institute for Public Policy.

by reading history. But because the future has not happened, our expectations of it can only be guesswork. Historically guided guesswork should perform better than one that knows no yesterdays.”⁵

Military strategic planning documents have always maintained that the future is unpredictable, and the weight behind this idea has increased steadily over the past decade. The 2005 NDS said that “we can identify trends but cannot predict specific events with precision,”⁶ and the 2006 National Security Strategy talked of hedging “in case states choose unwisely.”⁷ In his assessment of the 2006 QDR, Chairman of the Joint Chiefs of Staff (CJCS) General Peter Pace said “any attempt to predict the future security environment of 2025 is inherently difficult. Consider the challenge in 1985 of trying to characterize the security environment that would exist in 2006.”⁸ The 2008 Joint Operating Environment puts a much finer point on it.

The nature of the human condition will guarantee that uncertainty, ambiguity, and surprise will dominate the course of events. However carefully we think about the future; however thorough our preparations; however coherent and thoughtful our concepts, training, and doctrine; we will be surprised We will find ourselves caught off guard by changes in the political, economic, technological,

⁵ Colin S. Gray, "Why Strategy is Difficult," *Joint Forces Quarterly*, no. 22 (Summer 1999): 12.

⁶ DOD, *The National Defense Strategy of the United States of America*, (Washington, D.C., 2005), 2.

⁷ George W. Bush, *The National Security Strategy of the United States of America*, (Washington, D.C.: The White House, 2006), 36.

⁸ DOD, *Quadrennial Defense Review Report*, A-3.

strategic, and operational environments. We will find ourselves surprised by the creativity and capability of our adversaries.⁹

General J.N. Mattis, Commander of the U.S. Joint Forces Command, advised the current joint force to hold no illusions on the predictability of the future. “In our line of work, having the fewest regrets defines success when the shocks of conflict bring the surprise that inevitably accompanies warfare.”¹⁰

So other than unpredictability and the assurance of surprise, what can U.S. forces anticipate and plan against? Based on historical analysis and current trends there are a number of important items to consider, both in terms of the players and the techniques they may employ. First and foremost, “any enemy worth his salt will adapt to target our perceived weaknesses.”¹¹ The U.S. can rest assured that as it continues to develop capabilities, threats around the globe will consistently work, and possibly succeed in mitigating its advantages. This is an especially important point because acquisition and training have such long lead times, both for air and ground assets. The U.S. cannot wait until its enemies prove their ability to counter-balance their current technological superiority. The U.S. must prepare for this scenario while there is still time to generate and train fully capable S&R forces.

⁹ United States Joint Forces Command, *The Joint Operating Environment*, 3-4.

¹⁰ *Ibid.*, iv.

¹¹ *Ibid.*

In terms of possible threat players, Director of National Intelligence Mike McConnell noted that the U.S. must prepare its institutions for what he called the “profound threats of the times ... terrorists inside and outside the United States, nuclear proliferators, and rogue and failed states.”¹² The 2008 NDS expanded this list to include “violent transnational extremist networks, hostile states armed with weapons of mass destruction, [and] rising regional powers.”¹³

The NDS stressed that although DOD’s top priority was improving proficiency in “irregular warfare,”¹⁴ the U.S. cannot focus exclusively on such challenges. “Even though the likelihood of interstate conflict has declined in recent years, we ignore it at our peril. Current circumstances in Southwest Asia and on the Korean Peninsula, for example, demonstrate the continuing possibility of conflict.”¹⁵ The 2008 Defense Intelligence Strategy highlights that Chinese and Russian economic and military development are predominant factors over the coming decades. “China’s Gross Domestic Product (GDP) is slated to become second only to the United States. In Russia, defense spending during 2001–2007 has quadrupled and the military has stated plans to replace 45% of the army’s hardware by 2015.”¹⁶ There is clearly a vast array of international competitors that the U.S. must be prepared to contend with. But, in that S&R forces are

¹² Mike McConnell, “Overhauling Intelligence,” 58.

¹³ DOD, *The National Defense Strategy*, (2008), 1.

¹⁴ Ibid.

¹⁵ Ibid., 13.

¹⁶ DOD, *Defense Intelligence Strategy*, (Washington, D.C., 2008), 4.

capabilities-based, not threat-based, the capabilities that these competitors bring to bear are far more important than the players themselves.

The rise in global interdependence and technology proliferation requires the U.S. to prepare for a broad range of capabilities. During the Cold War, the U.S. maintained the lead in technological innovation in areas such as weapon systems, computers, and satellite technology. However, over the last 20 years “its lead has dwindled as innovation has moved from the public to the private sector and technological know-how has spread across the world. Worse still for the United States, its adversaries have been quick to adapt to technological improvements.”¹⁷ This means that American enemy capabilities will “range from explosive vests worn by suicide bombers to long-range precision-guided cyber, space, and missile attacks.”¹⁸ In order to define the role of the S&R community against this broad array of capabilities, this thesis categorizes the threat capabilities identified in U.S. strategic documents into two broad areas: conventional, and disruptive.

Despite the desire by many to dismiss conventional threats, they are a plausible and potential near-term reality. Based on a per capita GDP, many countries will have the ability to field large conventional militaries in the coming decades; in fact, the global trend is one of substantial potential rearmament.¹⁹ While these forces may not be globally

¹⁷ Mike McConnell, "Overhauling Intelligence," 56.

¹⁸ United States Joint Forces Command, *The Joint Operating Environment*, 3.

¹⁹ *Ibid.*, 25.

deployable, they could quickly affect a given region and “could significantly challenge the ability of the United States to project military force into their area.”²⁰

It is also conceivable that combinations of regional powers with sophisticated regional capabilities could band together to form a powerful anti-American alliance. It is not hard to imagine an alliance of small, cash-rich countries arming themselves with high-performance long-range precision weapons. Such a group could not only deny U.S. forces access into their country, but could also prevent American access to the global commons at significant ranges from their borders.²¹

The 2008 NDS maintains that the defense department must be able to defeat an enemy force that employs a full scale of capabilities, from conventional to irregular and kinetic to non-kinetic; “We must maintain the edge in our conventional forces.”²² Conventional conflicts would encourage threat forces to use capabilities against the U.S. that they may be reluctant to use at present. It is the potential loss of the global commons, particularly space that poses the most risk to the current U.S. S&R apparatus. Such a scenario could paralyze U.S. air and space-based S&R forces, which even for a short time, would be disastrous on the battlefield.

It is the disruption and possible paralysis of a space-dependant system that is the Achilles heel of the current S&R structure. “The use of asymmetric warfare techniques

²⁰ Ibid.

²¹ Ibid., 26.

²² DOD, *The National Defense Strategy*, (2008), 13.

such as denial and deception has become increasingly popular among potential adversaries as a means to counter U.S. and allied ISR and power projection capabilities.”²³ The development and proliferation of anti-access technology and weapons is a concern because they can restrict U.S. freedom of action, and “in some instances, we may not learn that a conflict is underway until it is well advanced and our options limited.”²⁴ These disruptive activities primarily affect information technologies, high-resolution imagery, and global positioning systems. Anti-access technology is relatively cheap and commercially available as dual-use civilian technologies, which are accessible to a wide range of state and non-state actors.²⁵ The global availability and potential deniability of dual-use technologies allows regional powers to develop capabilities for disruptive action without the traditional buildup warning indicators.²⁶

An example of one such surprise that could prove deadly to U.S. forces would be the development and use of electro-magnetic pulse (EMP) weapons. While commonly associated with nuclear detonations, the employment of non-nuclear EMP weapons could forever alter operational and technological discussions.

They are being developed, but are joint forces being adequately prepared to handle such a threat? The impact of such weapons would carry with it the most serious potential consequences for the communications,

²³ DOD, *Joint Publication 2-01*, I-2.

²⁴ DOD, *The National Defense Strategy*, (2008), 4.

²⁵ DOD, *The National Military Strategy*, 6.

²⁶ DOD, *Joint Publication 2-01*, I-2.

reconnaissance, and computer systems on which the Joint Force depends at every level.²⁷

Consider the effects on U.S. S&R activities if such a weapon were used in space.

“As with the profusion of inexpensive precision weapons, technological advances and increasing wealth will place the ability to conduct military operations in space within the reach of an increasing number of players.”²⁸ While the U.S. has enjoyed unchallenged dominance in space operations for decades, the playing field is leveling due to increased “proliferation of launch and satellite capabilities, as well as the development of anti-satellite capabilities.”²⁹ Senior leaders are conscious of this threat, as demonstrated by the 2008 Defense Intelligence Strategy (DIS). It identified as a strategic objective the elimination of “any advantage held by our adversaries to operate from and within the space and cyber domains.”³⁰ As shown in this DIS objective, any discussion of the potential disruption of space-based systems is inextricably linked to the fourth global common: cyberspace.

Though the volumes of debate surrounding what has been called the cyber-war are outside the scope of this paper, its potential disruptive effects for the U.S.’s S&R capability are worthy of note. Despite the legion of experts working diligently to maintain U.S. cyber security, the U.S. is accepting significant risk if it assumes that military

²⁷ United States Joint Forces Command, *The Joint Operating Environment*, 38-39.

²⁸ *Ibid.*, 23.

²⁹ *Ibid.*

³⁰ DOD, *Defense Intelligence Strategy*, 19.

secrets will always remain secret. “Small groups or individuals ...can attack vulnerable points in cyberspace ... compromising sensitive information and materials, and interrupting critical services such [as] ... information networks.”³¹ As addressed in the Comprehensive National Cybersecurity Initiative, “cyberspace has become a vital national interest economically, militarily and culturally, and the current patchwork of passive defense is likely to fail in the face of greater vulnerabilities and more sophisticated threats.”³²

Advances in automation and information processing pose a significant risk to U.S. operations, both at home and abroad. “Software tools for network-attack, intrusion and disruption are globally available over the Internet, providing almost any interested adversary a basic computer network exploitation or attack capability.”³³ As this paper will demonstrate in the China case study, with nearly every component of the S&R community relying on secure cyber links, the U.S. is operating with a possible single point of failure.

In summary, S&R forces must be prepared to function in an unpredictable and often amorphous operational environment. A virtually endless list of possible aggressors exists, collectively representing the full scope and scale of military capabilities – each working to defeat U.S. capability. The more sophisticated military opponents could

³¹ DOD, *The National Defense Strategy*, (2008), 7.

³² DOD, *Defense Intelligence Strategy*, 19.

³³ DOD, *The National Military Strategy*, 6.

mount “attacks on computers, space, and communications systems [that] will severely degrade command and control of U.S. forces. Thus, those forces must possess the ability to operate effectively in degraded conditions.”³⁴ The ability to continue S&R operations after contact and while degraded is a critical component of this analysis.

Sensor Allocation Criteria

“The foremost challenge of collection management is to maximize the effectiveness of limited collection resources within the time constraints imposed by operational requirements.”³⁵ While JP 2-01 seems to focus purely on aerial S&R assets, this same challenge holds true for the gamut of systems addressed in this paper. An analysis of the doctrinal criteria used by intelligence collection managers provides a good baseline for understanding asset applicability on the battlefield. Thus, JP 2-01 provides two primary considerations for sensor allocation criteria; sensor capability factors and battlefield factors.

Sensor capability factors are technical or performance characteristics including range, dwell time, and timeliness.³⁶ These factors translate into specific capabilities and limitations that are then considered, along with asset availability, to determine whether the system is even technically capable of performing the mission. The collection manager

³⁴ Ibid., 43.

³⁵ DOD, *Joint Publication 2-01*, III-11.

³⁶ Ibid., III-18.

compiles a preliminary list of available sensors and then compares them with a set of battlefield factors to determine final tasking selection.

Battlefield factors include threat, weather, terrain, and contamination.³⁷ The threat factor considers an asset's potential vulnerability to adversarial countermeasures, with respect to both the sensor and the platform. Weather and light conditions in and around the collection area affect sensor

capability, particularly with IMINT systems. Terrain constraints address possible masking issues and platform scan/pan capabilities. Contamination factors consider an asset's vulnerability to battlefield and WMD contaminants, as well as its ability to withstand

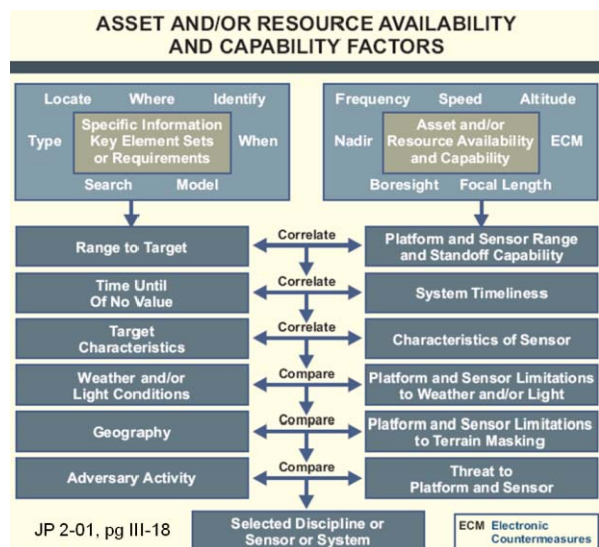


Figure 7: Asset Capability Factors

decontamination and potential for spreading the contaminant. Figure 7 diagrams the sensor application considerations and serves as a doctrinal baseline for the asset assessments throughout the remainder of this chapter.

³⁷ Ibid., III-19.

Terrain Constraints

This section evaluates asset capability with respect to key terrain challenges in predicted conflicts. These assessments are considered in a permissive environment unless otherwise noted.

Densely Wooded/Jungle

Jungle and densely wooded terrain has always been challenging terrain for armed conflict. Military historian Max Boot notes that in the jungles of Vietnam the U.S. attempted to overcome jungle challenges through industrial means, comparing the two competitors to the “Jetsons” and the “Flintstones.”³⁸ Boot uses an example of the Vietcong defeating the helicopter-mounted XM-2 personnel detector by hanging buckets of urine in trees.³⁹ This is a crude but efficient example of the deception and denial techniques available to even the most underdeveloped adversaries. As seen below in Figure 8, densely wooded/jungle terrain primarily limits those assets that rely on EO/IR sensors. While few SAR systems are capable of penetrating forest foliage, the matrix reflects the possibility of upgrades due to current radar technology studies.

³⁸ Max Boot, *The Savage Wars of Peace: Small Wars and the Rise of American Power*, (New York: Basic Books, 2002), 300.

³⁹ Ibid.

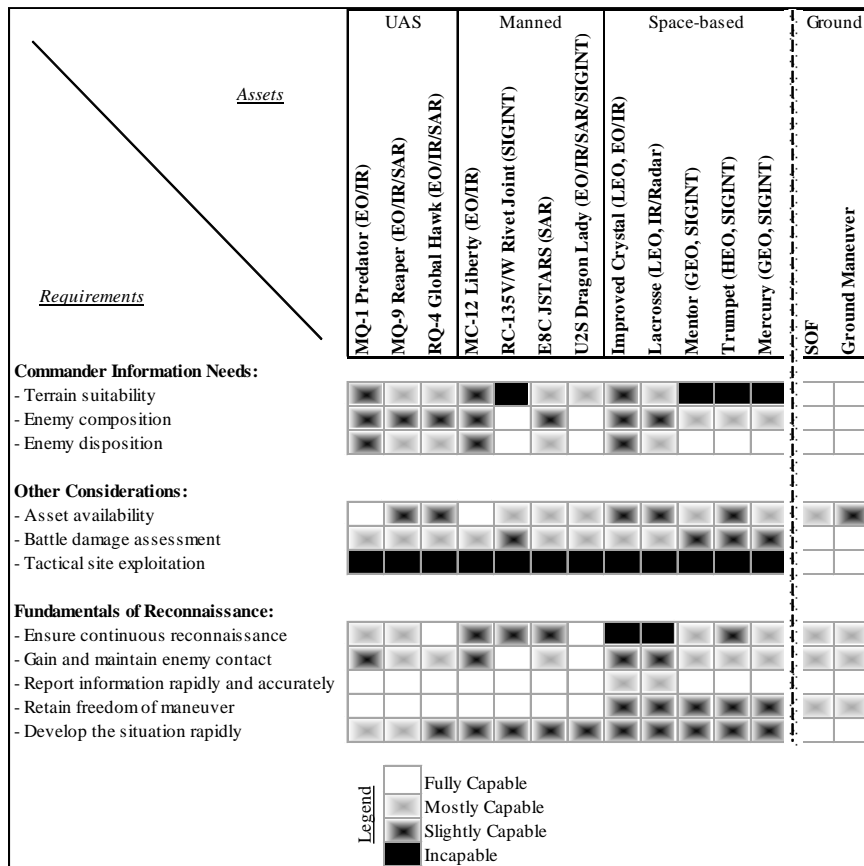


Figure 8: S&R Asset Comparison in Densely Wooded/Jungle Terrain

Operations in a wooded/jungle environment significantly degrade the capabilities of the air space-based S&R platforms, thus increasing the relative collection burden to ground-based capabilities. Effective collection options are essentially limited to ground and radar/SIGINT equipped aerial and space systems. In a non-permissive environment, the commanders' willingness to accept system loss could reduce the available options dramatically.

Mountainous

As Figure 9 shows, the limiting S&R factors in mountainous terrain are mobility and the masking effects of terrain height and shadows. U.S. Army Major General Franklin Hagenbeck, Commanding General of CJTF Mountain in Afghanistan, said that

due to rough terrain and weather “it was very difficult for our overhead ISR platforms to identify the cave complexes. So it took ‘boots on the ground’ to find the caves. The shadows, alone, precluded our discovering a cave until our Soldiers were almost on top of it.”⁴⁰ Military strategist Dr. Norman Friedman wrote that while space-based systems were significantly limited due to orbits and system capabilities, lower-flying aircraft proved far more useful. “The problem was analogous to one encountered in the Gulf War, when the best surveillance systems, mainly satellites, seemed to operational commanders not to be responding to their needs.”⁴¹

⁴⁰ Robert H. McElroy, "Afghanistan, Fire Support for Operation Anaconda," *Field Artillery*, September/October 2002, 5-6.

⁴¹ Norman Friedman, *Terrorism, Afghanistan, and America's New Way of War*, (Annapolis: Naval Institute Press, 2003), 168-169.

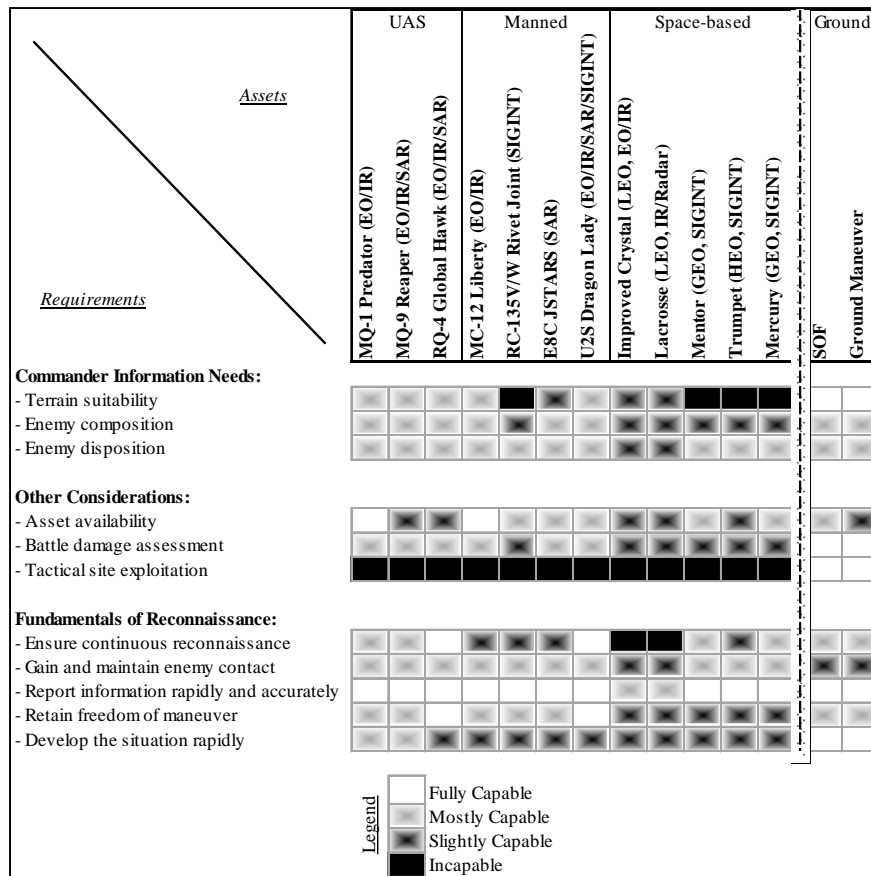


Figure 9: S&R Asset Comparison in Mountainous Terrain

Mountainous terrain severely limits space-based effectiveness and ground mobility. In the permissive environment reflected in Figure 9, both unmanned and manned aerial systems provide the greatest capability. However, due to flight pattern requirements, a non-permissive environment requires the commander to accept a higher potential of system loss when using any aerial systems other than the RQ-4 and U2.

Urban

Akin to the mountainous terrain challenges, S&R in urban terrain centers on abilities to negotiate the density and varied structural heights; from subsurface to supersurface. More importantly, urban terrain requires assets to interact with the occupying population. Colonel Howcroft notes that while aerial assets can often provide

high resolution images of individual buildings, “we still cannot see who is inside, whether he is armed, or if he is hostile. It requires a man on the ground to go into the building or to communicate face-to-face with the inhabitants of the neighborhood to collect and evaluate the intelligence.”⁴²

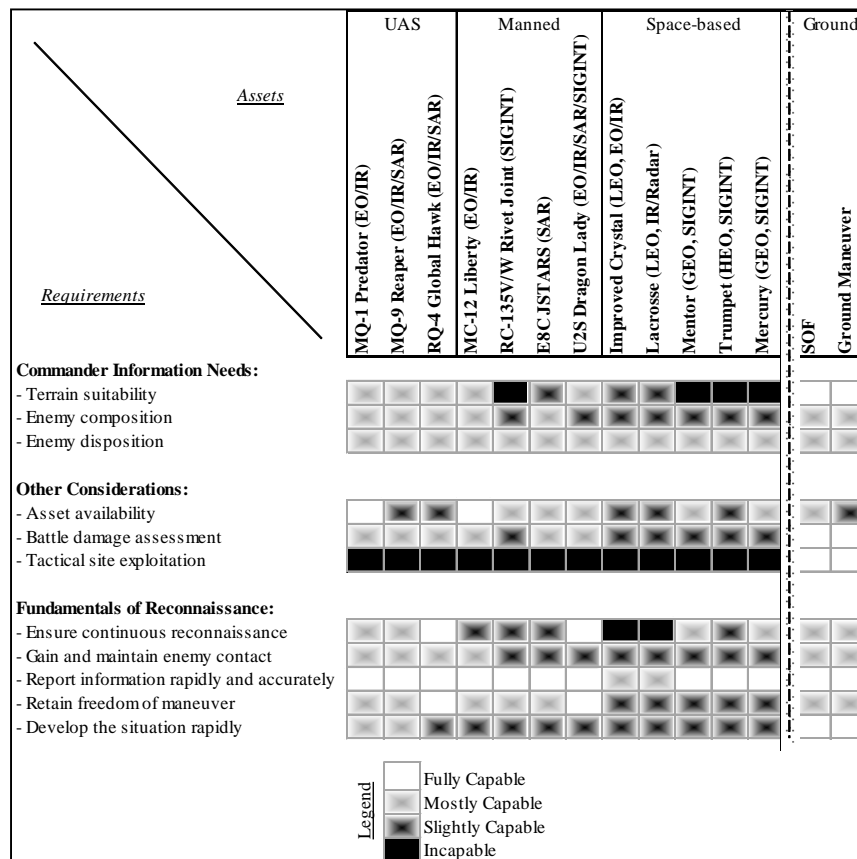


Figure 10: S&R Asset Comparison in Urban Terrain

Figure 10 shows that even in a permissive urban environment, space-based systems are often of limited utility with regard to an operational commander’s CCIR. To

⁴² James R. Howcroft, "Technology, Intelligence, and Trust," 22.

slightly varying degrees, the ground, unmanned and most manned systems remain feasible in both permissive and non-permissive environments. The discriminating factor is the urban population. In nearly all circumstances, the U.S. must use ground S&R forces in order to effectively answer CCIR in urban terrain.

Weather Constraints

Weather affects both the platform and its sensor capabilities. It affects a platform's ability to operate in inclement conditions, such as lightning and ice storms. It also impacts a sensor's ability to observe through natural constraints such as clouds and rain, as well as battlefield obscurants such as smoke, fire, and dust.

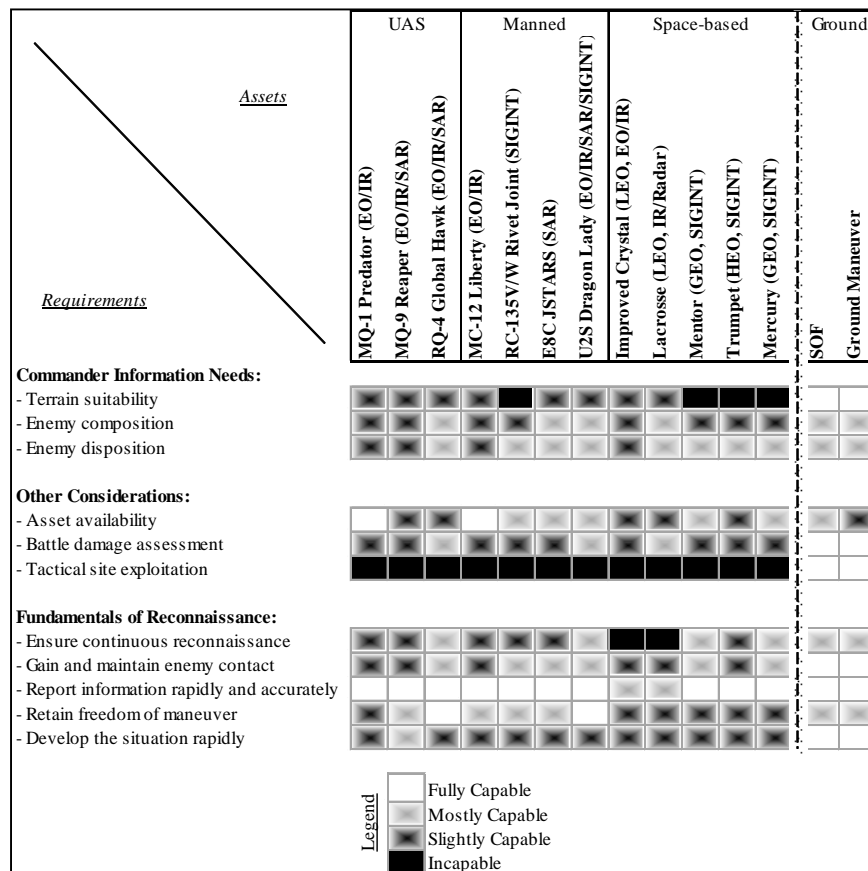


Figure 11: S&R Asset Comparison with Weather Constraints

As evident in Figure 11, weather severely limits most air/space-based systems. Only those that can operate above storm ceilings and have radar to attempt signal penetration can function during most inclement weather conditions. This fact exacerbates the results of the prior terrain analysis, because inclement weather conditions can exist in each of the terrain scenarios. A forested region with routine cloud cover and periodic rain storms would negate the capabilities of all but a few of the total available systems.

Threat Constraints

At this point the reader is intuitively able to recognize the network-dependency of air/space-based systems. While ground-based systems are also highly dependent on network viability, they remain combat capable without it; albeit in a degraded capacity. It is the consequences of network disruption that links the preceding system capabilities section with the following discussion of threat capabilities.

Terrain and weather impact U.S. capabilities in relatively predictable ways; this is not always the case with threat forces. The only constant is that opposing forces will always seek to mitigate U.S. advantages, particularly with respect to the military. Just as the USSR counter-balanced U.S. power by creating their own nuclear weapon, threat forces will eventually find a way to match or beat U.S. capabilities.

Traditional threat capabilities are well known and need no description here. However, history does provide examples of threat ingenuity that warrants consideration for even modern-day S&R systems. Both examples show that the most secure U.S. systems are within reach of threat forces should they decide to act against them.

The first example takes place on 1 May, 1960. A then classified U2 Dragon Lady flew from Peshawar destined for Bodo, Norway, and was to photograph two Russian

intercontinental ballistic missile sites enroute. Both sites were known to be surrounded by heavy anti-aircraft systems. As the U2 approached Sverdlovsk, flying at 67,000 feet, the Soviets volley-fired 14 SA-2 surface-to-air missiles. Although the missiles were clearly unable to reach that altitude, “the aircraft disintegrated in the shock waves caused by the exploding missiles.”⁴³

In the second example, occurring in 2007, the Chinese government used an interceptor missile to destroy one of their low earth orbit satellites.⁴⁴ While this incident is discussed in greater detail in the next chapter, it is pertinent here to illustrate demonstrated threat capabilities. Author T.W. Lee⁴⁵ states that this incident represents just a small fraction of the plausible current threats to space-based systems. Using global missile defense systems as one example, Lee demonstrates that the dual use nature of the weapon allows them to track and destroy space satellites; both from the ground and in space. “Some of the missile kill devices under development are designed to be placed in orbit ... it would be a relatively simple matter to point and shoot at the relatively slow-moving satellites in the vicinity.”⁴⁶

⁴³ GlobalSecurity.org, *Military, Systems, Aircraft*, SENIOR YEAR / AQUATONE / U-2 / TR-1.

⁴⁴ United States Joint Forces Command, *The Joint Operating Environment*, 23.

⁴⁵ T.W. Lee is Associate Professor of Mechanical and Aerospace Engineering at Arizona State University.

⁴⁶ T.W. Lee, *Military Technologies of the World*, 218.

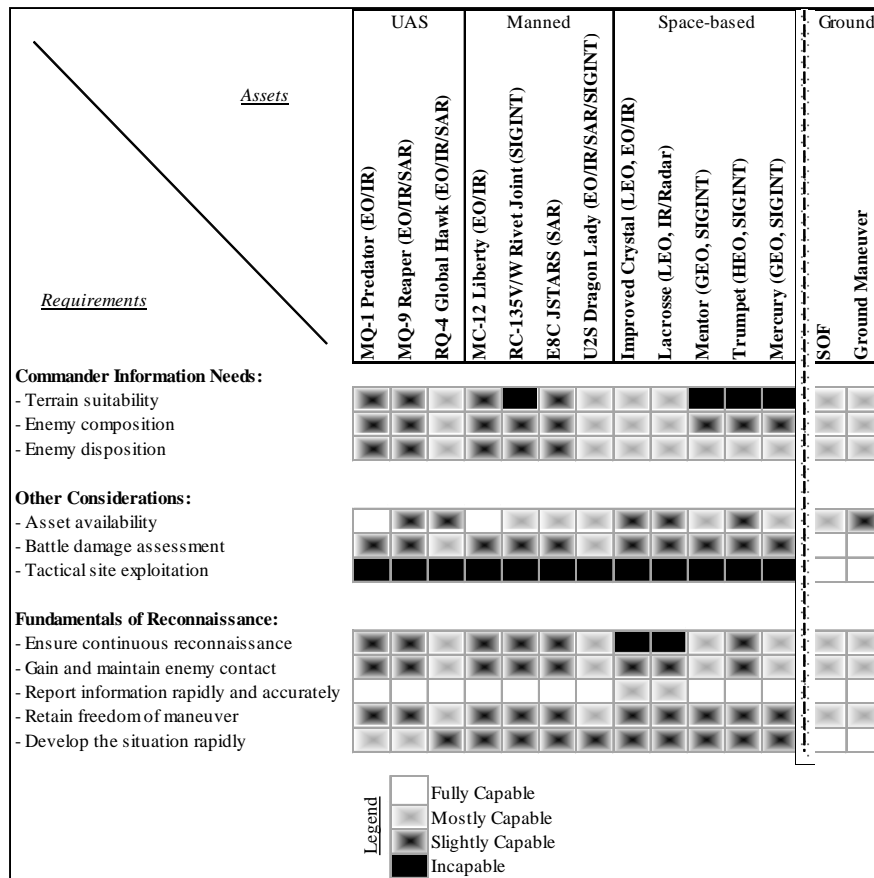


Figure 12: S&R Asset Comparison with Threat Constraints

Operational commanders have a plethora of S&R assets available. In a permissive environment, regardless of terrain, he can mix and match them in any number of ways to mitigate the limitations of each system. However, adding the complexities of weather to terrain exacerbates many system limitations. Further adding threat constraints, on top of both terrain and weather, removes most S&R options all-together. Based on the operational environment discussed at the beginning of the chapter, the U.S. is not currently in an advantageous position to conduct effective non-permissive S&R operations. The China case study in the next chapter will highlight the S&R challenges should the U.S. have to fight an organization with the capabilities resident in the Chinese government.

CHAPTER 4

CHINA: A THREAT CASE STUDY

For every analyst that identifies China as a near-term and tangible threat to U.S. national security, there is one that dismisses that possibility outright. This section is not intended to weigh in on that debate. It is, however, intended to demonstrate the capabilities resident inside one country, and the potential impacts on S&R forces. U.S. strategic documentation on China provides but one example of how a potential adversary is planning to capitalize on the current imbalance in U.S. S&R capabilities.

The 2006 QDR reports that since 1996 the Chinese have maintained a 10% annual increase in defense spending,¹ and this is a potential risk to U.S. national security. “Of the major and emerging powers, China has the greatest potential to compete militarily with the United States and field disruptive military technologies that could over time offset traditional U.S. military advantages absent U.S. counter strategies.”² Echoing this concern, the 2009 DOD assessment of China said that “of all foreign intelligence organizations attempting to penetrate U.S. agencies, China’s are the most aggressive.”³ Their intelligence services “pose a significant threat both to the national security and to

¹ Due to its labor market and reverse engineering the latest technologies, the Chinese spend an order of magnitude less on its equipment than does the U.S.; particularly in space programs. United States Joint Forces Command, *The Joint Operating Environment*, 50.

² DOD, *Quadrennial Defense Review Report*, 29.

³ DOD, “Military Power of the People’s Republic of China, 2009,” Annual Report to Congress, (Washington, D.C., 2009), 38.

the compromise of U.S. critical national assets ... [and they] will remain a significant threat for a long time.”⁴

Showing concern over this development, the 2006 National Security Strategy states that the U.S.’s “strategy seeks to encourage China to make the right strategic choices for its people, while we hedge against other possibilities.”⁵ This thesis shows that the U.S. is hedging in the wrong direction.

U.S. Army Lieutenant General Keith Alexander, Director of the National Security Agency, defined cyberspace as a critical component of the Chinese threat. “Nations such as China and Russia are developing their own ‘cyberspace warriors.’ China, for instance, has formed cyberspace battalions and regiments, the primary purpose of which is to identify and exploit weaknesses in our military, government, and commercial networks.”⁶ This fact is troubling with the bulk of U.S. S&R capability inextricably linked to networked and space-based backbones that are particularly vulnerable to cyberspace attacks.

In line with a perpetual cyber threat, Chinese military writings emphasize the development of innovative strategies and tactics to balance the capabilities of technologically superior opponents.⁷ “The Chinese are working hard to ensure that if

⁴ Ibid.

⁵ George W. Bush, *The National Security Strategy*, (2006) 41-42.

⁶ Keith B. Alexander, "Warfighting in Cyberspace," *Joint Forces Quarterly*, no. 46 (3rd Quarter 2007): 59.

⁷ DOD, "Military Power of the People's Republic of China, 2009," 16-17.

there is a military confrontation with the United States sometime in the future, they will be ready.”⁸ The Chinese military stresses that battlefield success depends on the seizure of electromagnetic dominance at the beginning of a campaign.⁹ To that end, China is hardening its own capabilities by moving communications infrastructure to fiber¹⁰ and is developing counter-space, anti-radiation, and advanced integrated air defense systems to deny these capabilities to an opponent.¹¹ This means that U.S. aerial and space-based systems would, for perhaps the first time, need to operate against an opponent both capable and intent on mitigating their effectiveness.

The 2008 NDS maintained that in addition to cyber and information warfare attacks, China is likely to continue expanding its conventional military capabilities. Most germane to this topic is their focus on space and anti-satellite capabilities.¹² A People’s Liberation Army (PLA) analysis of U.S. and coalition military operations reinforced the importance of operations in space. They identified that battlefield monitor and control, information communications, navigation and position, and precision guidance all rely on satellites and other sensors. PLA writings emphasize the necessity of “destroying, damaging, and interfering with the enemy’s reconnaissance/observation and

⁸ United States Joint Forces Command, *The Joint Operating Environment*, 27.

⁹ DOD, "Military Power of the People's Republic of China, 2009," 14.

¹⁰ Ibid., VIII.

¹¹ DOD, *Quadrennial Defense Review Report*, 29-30.

¹² DOD, *The National Defense Strategy*, (2008), 3, 22.

communications satellites,”¹³ suggesting that such systems, as well as navigation and early warning satellites, could be among initial targets to “blind and deafen the enemy.”¹⁴

“China’s nuclear arsenal has long provided Beijing with an inherent ASAT [anti-satellite] capability.”¹⁵ However, the January 2007 Chinese test of an interceptor missile “made clear their belief that space was a potential theater of conflict and that they aimed to possess the capability to fight in that environment.”¹⁶ By successfully destroying one of their weather satellites using a direct-ascent ASAT missile,¹⁷ China demonstrated its ability to attack satellites in low earth orbit;¹⁸ remember that all U.S. optical and radar satellites are in a low earth orbit. “The direct-ascent ASAT system is one component of a multi-dimensional program to limit or prevent the use of space-based assets by potential adversaries during times of crisis or conflict.”¹⁹

China is also developing the ability to “jam, blind, or otherwise disable satellites and their terrestrial support infrastructure.”²⁰ China already has the ability to jam common satellite communications and GPS receivers, and is currently developing

¹³ DOD, “Military Power of the People’s Republic of China, 2009,” 13-14.

¹⁴ Ibid.

¹⁵ Ibid., 27.

¹⁶ United States Joint Forces Command, *The Joint Operating Environment*, 23.

¹⁷ This event created a debris field that makes that portion of space unusable throughout the decades it will take for all remnants to deorbit. For more information on this event as well as in depth discussions of space warfare, (such as dual-use missile defense technologies and nuclear explosions in space) see Wilson W.S. Wong and James Fergusson, *Military Space Power: A Guide to the Issues*, Santa Barbara, CA: ABC-CLIO, LLC, 2010, 93.

¹⁸ DOD, “Military Power of the People’s Republic of China, 2009,” 27.

¹⁹ Ibid., 27.

²⁰ Ibid., 14.

additional kinetic and directed-energy ASAT options, such as lasers, high-powered microwaves, and particle beams. “Citing the requirements of its manned and lunar space programs, China is improving its ability to track and identify satellites – a prerequisite for effective, precise counterspace operations.”²¹

While there are a number of factors that lead many to discount a Chinese threat to the U.S., such as a burgeoning middle class and an artificially inflated economy, both sides of the debate must remember that the threat to U.S.’s S&R capability comes not from China itself, but from the capabilities it represents. China maintains only a limited capability to sustain military power at great distances, “but its armed forces continue to develop and field disruptive military technologies, including those for anti-access/area-denial, as well as for nuclear, space, and cyber warfare, that are changing regional military balances and that have implications beyond the Asia-Pacific region.”²² Evidence shows that China develops these systems both for their own use as well as for global export,²³ thus enabling other nation-states and regional cooperatives to pose similar threats to U.S. capabilities.

²¹ Ibid., 27.

²² Ibid., I.

²³ DOD, *Quadrennial Defense Review Report*, 29-30.

CHAPTER 5

CONCLUSION

This study showed that Department of Defense (DOD) overdependence on air and space-based sensor technologies reduces the surveillance and reconnaissance (S&R) capability of the operational-level commander and sets the conditions for initial failure on the future battlefield.

An analysis of DOD capability priorities from 1950 to present shows a steady increase in reliance on technological solutions coupled with reduced manpower. This trend was seemingly justified at the conclusion of the Cold War and in the overwhelming success of U.S. forces in Operation Desert Storm. Throughout the second tenure of Donald Rumsfeld as Secretary of Defense, this technological focus gained new impetus within his vision of department-wide transformation.

This transformation, more than just improving capabilities, fundamentally changed how DOD viewed the conduct of war. Through concepts such as the Revolution in Military Affairs, Net-Centric Warfare, and Information Dominance, DOD sought to remove the fog and friction of war by trading information for mass. Analysis shows that transformation was not necessarily a bad concept, but was flawed in its extreme interpretations and subsequent execution. “The quest for technological superiority, like

anything else, carries a cost; and that if this cost is not carefully studied and managed it may increase to the point where the adverse effects exceed the beneficial ones.”¹

Analyzing the capabilities and limitations of DOD’s current and predicted S&R force reveals a wide disparity between ground and air/space-based systems. Further assessing these systems against battlefield constraints reveals an S&R force structure that, while functional in a permissive environment, will not perform as advertised against plausible future threat scenarios.

The U.S. should always strive to maintain technological superiority over future opponents, but not at the cost of creating an exploitable gap in battlefield capability. The predictable effects of terrain and weather on S&R systems highlight the current and projected limitations across the S&R force. When threat capabilities are applied, however, it becomes evident that many U.S. air/space-based systems are no longer assured as options to answer the operational commander’s CCIR. Yet it is on the assumption that these platforms will provide full-spectrum information dominance that justified the decades-long degradation in ground S&R capabilities.

Many potential adversaries currently possess the ability to negate U.S. S&R capabilities. While it is never too late to fix a problem, DOD must first acknowledge that a problem exists. Ground S&R assets, particularly at the Army Corps/Marine

¹ Martin L. Van Creveld, *Technology and War: From 2000 B.C. to the Present*, 231-232.

Expeditionary Force, and Army Division/Marine Expeditionary Brigade level, must return to time tested and historically justified capabilities if the U.S. is to avoid future mission failure or unnecessary loss of life and treasure. “In the end, our enemies will not outfight us. We’ll muster the will to do what must be done – after paying a needlessly high price in the lives of our troops and damage to our domestic infrastructure. We will not be beaten, but we may be shamed and embarrassed on a needlessly long road to victory.”²

² Ralph Peters, "The Counterrevolution in Military Affairs," 19.

APPENDIX A

OPERATIONAL INFORMATION REQUIREMENTS

“If you know the enemy and know yourself, you need not fear the result of a hundred battles ... What is called ‘foreknowledge’ cannot be elicited from spirits, nor from gods, nor by analogy with past events, nor from calculations. It must be obtained from men who know the enemy situation.”¹

This appendix discusses the commander’s information needs at the operational level of war. The first section describes a series of fundamental concepts needed to understand the operational commander, and is followed by a review of operational-level information needs. The final section analyzes the DOD view of intelligence collection focus. At the conclusion of the appendix, the reader should have an understanding of the types of information needed at the operational level of war.

Fundamental Concepts

What does the operational commander need to know? In order answer this question one must generally understand some implied concepts within the question itself; namely the operational level of war and the operational commander. According to Joint Publication (JP) 1-02, the operational level of war links “tactics and strategy by establishing operational objectives needed to achieve the strategic objectives, sequencing

¹ Sun Tzu, *The Art of War*, Translated by Samuel B. Griffith (London: Oxford University Press, 1963), 145.

events ... initiating actions, and applying resources to bring about and sustain these events.”² As straightforward as this may seem, the discussion gets a bit more complicated when combined with the role of an operational commander, such as U.S. Combatant Commanders (CCDRs). In JP 3-0, “Combatant commanders are the vital link between those who determine national security policy and strategy and the military forces or subordinate JFCs that conduct military operations.”³

It would be overly-simplistic to leave their role as merely bridging strategy to tactics. As noted by Dr. Paul Melshen, professor at the Joint Forces Staff College, “Every military officer who attends his respective staff college and war college knows that strategy evolves from political policy, and not vice versa.”⁴ JP 3-0 refines this point: “Based on guidance from the President and [Secretary of Defense], CCDRs develop strategies that translate national and multinational direction into strategic concepts or courses of action (COAs) to meet strategic and joint operation planning requirements.”⁵ Thus the CCDR is fully aware that if his theater strategy is to succeed, it must be based on sound political policy and DOD strategy.

² DOD, *Joint Publication 1-02, DOD Dictionary of Military and Associated Terms* (Washington, D.C., 2009), 399.

³ DOD, *Joint Publication 3-0, Joint Operations* (Washington, D.C., 2008), x.

⁴ Paul Melshen, "Mapping Out a Counterinsurgency Plan: Critical Considerations in Counterinsurgency Campaigning," *Small Wars and Insurgencies* 18, no. 4 (December 2007), 668.

⁵ DOD, *Joint Publication 3-0*, x.

This discussion is critically important to an analysis of S&R capability because a CCCR's assessment of information needs can vary wildly from those making decisions on collection asset acquisition and allocation. As noted in the 2006 QDR, "Changes should focus on meeting the needs of the President of the United States and joint warfighting forces, represented by the Combatant Commanders."⁶ It is worthy to note that there is a circular, 'chicken-and-egg' relationship between policy and strategy that is both necessary and healthy. However, years in both Afghanistan and Iraq prove that operational commanders often create and execute plans without the guidance that is supposed to form the base of their strategy.

Armed with a basic understanding of the operational level of war as well as the role of the operational commander, the line of thinking returns to the premise question – what does the operational commander need to know? While DOD doctrine does not directly answer this question, it does provide some insights. All italicized items within the next section highlight areas of probable information need.

Doctrinal Review

As referenced in Figure 13, JP 2-0 highlights the intelligence requirements across the three levels of war. The remainder of this section will build on this structure and

⁶ DOD, *Quadrennial Defense Review Report*, 1.

discuss doctrinal information insights of the commander from initiation of strategy to execution of combat operations.

Prior to the execution of armed combat, CCDRs information needs center on the creation and maintenance of his respective theater strategy. JP 3-0 states that “Theater strategy is determined by CCDRs based on analysis of changing events in the operational environment and the development of options to set conditions for success.”⁷ JP 2-0 further clarifies the role of

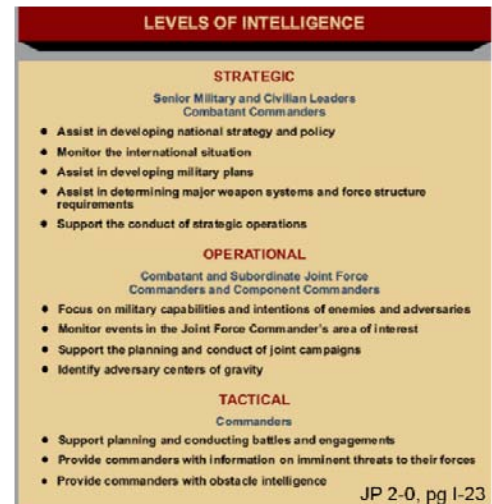


Figure 13: Levels of Intelligence

intelligence operations during campaign planning as a “focus on providing ... [the] information required to *identify the adversary's centers of gravity*,⁸ *COAs [course of action]*, and *high-value targets*.”⁹ Two of the planning tools that support development of the theater strategy, the strategic estimate and operational design, also provide insights into doctrinal intelligence needs. While it is outside the scope of this paper to fully explain these concepts, they are useful in highlighting the information needs that exist at the operational level.

⁷ DOD, *Joint Publication 3-0*, xi.

⁸ The Center of Gravity is “the source of power that provides moral or physical strength, freedom of action, or will to act.” Its critical factors, or components, are Critical Capabilities, Critical Requirements, and Critical Vulnerabilities. DOD, *Joint Publication 1-02*, 81.

⁹ DOD, *Joint Publication 2-0, Joint Intelligence* (Washington, D.C., 2007), xi.

The CCDR and his staff use the strategic estimate to develop their theater strategic concepts and joint campaign/operation plans. The CCDR develops his strategic estimates “after reviewing the operational environment, *nature of anticipated operations*, and *national and multinational strategic direction*. In the strategic estimate, commanders *focus on the threat* and consider other circumstances affecting the military situation as they develop and analyze COAs.”¹⁰ More specifically, the strategic estimate considers “the *adversary’s likely intent and COAs*.”¹¹

Operational design is defined as “The conception and construction of the framework that underpins a campaign or major operation plan and its subsequent execution.”¹² From JP-1, “Operational design essentially involves *understanding strategic guidance, identifying the adversary’s centers of gravity and critical factors*, and developing an operational concept to achieve strategic objectives.”¹³

According to JP 2-01, when the command transitions from peacetime to wartime operations, “intelligence focuses on *enemy military capabilities, centers of gravity, and potential courses of action* to provide operational and tactical commanders the information they need to plan and conduct operations.”¹⁴

¹⁰ DOD, *Joint Publication 3-0*, xi.

¹¹ *Ibid.*, I-4.

¹² DOD, *Joint Publication 1-02*, 398.

¹³ DOD, *Joint Publication 1*, I-18.

¹⁴ DOD, *Joint Publication 2-01*, I-3.

Combining JP 5-0 planning guidance¹⁵ with the above doctrine shows that throughout the scope of conflict the operational commander needs to understand the following:

- operational environment and nature of anticipated operations
- national and multinational strategic direction and guidance
- political and military intentions and objectives with possible COAs
- enemy center of gravity with related critical factors
- enemy high value targets
- operational characteristics such as strength, composition, disposition; reinforcements; logistics; time, and space factors (including basing utilized and available); and combat/noncombat efficiency and proficiency in joint operations

One final information management concept is worthy of note, that of Commander's Critical Information Requirements (CCIR). "CCIRs comprise information requirements identified by the commander as being critical to timely information management and the decision-making process that affect successful mission accomplishment."¹⁶ Essentially CCIR allow the commander to prioritize the information required to make a decision. CCIRs account for the small size of the above list versus the gamut of information that is actually used by the commander and his staff to plan, decide and act.

¹⁵DOD, *Joint Publication 5-0, Joint Operation Planning* (Washington, D.C., 2006), B-2.

¹⁶ *Ibid.*, III-27.

It is important to remember that the levels of war are not mutually exclusive.

“Geographic CCDRs ... remain acutely aware of the impact of tactical events. Because of the inherent interrelationships between the various levels of war, commanders cannot be concerned only with events at their respective echelon, but must understand how their actions contribute to the military end state.”¹⁷ Colonel Howcroft notes that:

The tactical commander, immersed 24/7 in the cultural nuances of his local environment, is now, more than ever, in possession of the most accurate picture of the battlefield. It may be only a small piece, but just as operational success is an accumulation of tactical successes, so is an accurate intelligence picture at the operational level an accumulation of smaller, accurate intelligence pictures from below.¹⁸

In summary, the operational level commander operates in a complex and often ambiguous environment. While it is possible to derive a draft list of doctrinally sound information needs, it is understood that the commanders information requirements can vary based on any number of situations. And just as the information varies, so do the assets available. The commander depends on national S&R assets and subordinate tactical assets alike in order gain his needed intelligence.

¹⁷ DOD, *Joint Publication 3-0*, IV-15.

¹⁸ James R. Howcroft, "Technology, Intelligence, and Trust," 25.

APPENDIX B

DOD TECHNOLOGY CONCEPTS

This appendix assesses the DOD concepts of the “Revolution in Military Affairs” (RMA), Network-Centric Warfare (NCW), and Information Dominance/Dominant Battlefield Awareness. While inherent weaknesses in these concepts have contributed to their relative decline over the past several years, the appendix defines the fundamental concept behind each idea and describes their pervasive nature in terms of both past and current acquisition priorities; the effects of which remain prevalent in today’s service.

It is important to note the state of national affairs during the genesis of these ideas. These technology-centric concepts stem from a time when the military establishment experienced the fall of the Berlin Wall and the overwhelming victory in Operation Desert Storm. Couple these events with the emplacement of Donald Rumsfeld as Secretary of Defense in 2001 and the stage is set for a technological answer to military problems.

As demonstrated in the 2006 QDR, Secretary Rumsfeld established the precise environment needed to support a new “technological revolution”; an efficiency-minded business with centralized decision making authority. The QDR stated that the armed forces were “hampered by inefficient business practices Since 2001, the Department has moved steadily toward a more integrated and transparent senior decision-making

culture and process for both operational and investment matters [DOD] must undertake reforms to reduce redundancies.”¹ At the conclusion of this appendix, the reader will understand the pervasiveness of the DOD reforms and be able to identify their affects on current operations.

Revolution in Military Affairs

In their book on the subject, Harlan Ullman and James Wade defined RMA as “the phenomenon or process by which the United States continues to exploit technology to maintain [a] decisive force advantage, particularly in terms of achieving ‘dominant battlefield awareness’.”² In reality there have been a number of historical “revolutions in military affairs,” but all references to RMA in this paper refer to activities since 1980.

Author and retired U.S. Marine Colonel T.X. Hammes maintains that while RMA is not clearly defined, the discussion does focus on the “technological aspects of warfare – in particular, the military-technical revolution and how to quickly apply that ‘revolution’ to our forces, to assure our continued superiority in combat.”³

U.S. forces do not want a fair fight and the DOD should leverage every opportunity to maintain its edge. According to the 2008 National Defense Strategy, “Technology and equipment are the tools of the Total Force, and we must give our people

¹ DOD, *Quadrennial Defense Review Report*, 63, 65.

² Harlan Ullman and James Wade, Jr., *Shock & Awe: Achieving Rapid Dominance*, (Washington, D.C.: U.S. Government Printing Office, 1996), 4-5.

³ Thomas X. Hammes, *The Sling and the Stone*, 7.

what they need, and the best resources, to get the job done. First-class technology means investing in the right kinds of technology at the right time.”⁴ If the argument stopped here, there would be little issue from anyone in the defense community.

But, what of the general premise of technology driven military operations? Van Creveld says that warfare has always used technical devices. “However, the idea that war is primarily a question of technology ... that it should employ technologically-derived methods, and must seek victory by acquiring and maintaining technological superiority – that idea has been shown to be neither self-evident, nor necessarily correct, nor even very old.”⁵ Van Creveld goes on to note that this drive for technological superiority “is one of the most significant developments brought about by the advance of technology since the Industrial Revolution; when taken to extremes, it can also be one of the most dangerous.”⁶

Historian and scholar Michael Ignatieff writes that the core of RMA is a commander linked to precision munitions through the use of computers. “When linked up to surveillance satellites as well as spy planes, computers increase the information available to a commander ... if – a big if – this information can be digested and compressed into timely knowledge of the enemy’s dispositions.”⁷ Ignatieff goes on to

⁴ DOD, *The National Defense Strategy*, (2008), 19.

⁵ Martin L. Van Creveld, *Technology and War*, 312.

⁶ Ibid.

⁷ Michael Ignatieff, *Virtual War*, 171.

write that RMA “has aroused intense resistance in the U.S. armed forces [because] the new technology seems to accuse generations’ worth of procurement decisions ... [and] called into question the heavy industrial armies created to fight World War II.”⁸ He said that proponents of RMA would ask “If you have Cruise missiles, why do you need all those airplanes? If you have precision guided weapons launched from submarines, why do you need all those aircraft carriers and destroyers?”⁹

For the central claim of the new technological gospel was that computers, battlefield sensors and spy satellites could dispel the ‘fog’ of war ... and eliminate the ‘friction’ ... standing in the way of military victory. Generals like Norman Schwarzkopf were sceptical [sic] ... (knowing) that the ‘systems analysts’ of the Pentagon had promised (during Vietnam) that new technologies married to new tactics – the Huey helicopter re-equipped as a gunship – would dispel the fog and grease the friction of warfare. And they hadn’t.¹⁰

So the detractors of RMA seems to take issue not with a technologically enhanced force, but with the idea that a procurement focus on technology will eventually lead to an extreme condition where a smaller force would eventually count on the technology to overcome “fog,” “friction” and the realities of war. Military correspondent Michael Gordon and Lieutenant General (Retired) Bernard Trainor make this very point in their coverage of Operation Iraqi Freedom.

⁸ Ibid.

⁹ Ibid.

¹⁰ Ibid., 173.

The [Bush] administration put far too much confidence in American military technology, Special Operations Forces, and clandestine operations. Rumsfeld's principles of transformation were in large measure a codification of the long-promised 'revolution in military affairs' ... During the march to Baghdad, the approach was effective ... but after the fall of Baghdad ... military technology was less decisive against an opponent that faded away into Iraqi cities only to fight another day ... to gain control ... the United States needed more boots on the ground.¹¹

While it is clear that technological improvements have a rightful place in DOD procurement priorities, it is equally clear that misplaced priorities have had and will continue to have a deleterious effect on battlefield success. The 2008 JOE states that "The recent experiences of Afghanistan and Iraq have made clear that in war, human beings matter more than any other factor. There are other dimensions, including technology, that are important, but rarely decisive."¹²

Network-Centric Warfare

As RMA proposed a vision of technical solutions to warfare challenges, Network-Centric Warfare (NCW) was the medium to attain the vision. "The DOD's 'network-centric warfare' was first articulated by Vice Admiral Arthur Cebrowski and John Garstka¹³ in a 1998 article of the same name."¹⁴ Much like discussions surrounding the

¹¹ Michael R. Gordon and Bernard E. Trainor, *COBRA II: The Inside Story of the Invasion and the Occupation of Iraq*, (New York: Pantheon Books, 2006), 499-500.

¹² United States Joint Forces Command, *The Joint Operating Environment*, 48.

¹³ Vice Admiral Cebrowski served as the director of the Office of Force Transformation from 2001-2005. In this role, Admiral Cebrowski was an advocate for change across the armed forces, making policy recommendations directly to Secretary Rumsfeld. John Garstka was an Assistant Director within the Office

meaning of Effects Based Operations, not everyone in the defense arena uses NCW to mean the same thing. On one hand, NCW is simply the linking of assets together in order to achieve greater situational awareness and support command decisions; few would debate the usefulness of such an environment. However, this simplistic view does not properly define NCW as intended by its creators.

At its core, NCW is the ability to conduct warfare with fewer assets¹⁵ based on the assumption that decision makers have near-perfect battlefield knowledge¹⁶ and all elements of combat power are securely networked together¹⁷ with a near-instantaneous flow of information.¹⁸ However, because there is not a universally accepted definition for NCW, the following section highlights a series of official documents and statements supporting the above definition.

According to the 2003 Transformation Planning Guidance, DOD's goal was information age military forces that are "less platform-centric and more network-centric ... able to distribute forces more widely by increasing information sharing via a secure network that provides actionable information at all levels of command."¹⁹ Admiral

of Force Transformation, with focus on Concepts and Operations. Together these men were outspoken advocates for NCW.

¹⁴ Thomas X. Hammes, *The Sling and the Stone*, 7.

¹⁵ Arthur Cebrowski, "Speech to the Network Centric Warfare 2003 Conference."

¹⁶ Harlan Ullman and James Wade, Jr., *Shock & Awe*, 4-5.

¹⁷ DOD, "Transformation Planning Guidance," (Washington, D.C., 2003), 9.

¹⁸ Arthur Cebrowski, "Speech to the Network Centric Warfare 2003 Conference."

¹⁹ DOD, "Transformation Planning Guidance," 9.

Cebrowski further defined NCW as “information superiority-enabled concept of operations ... In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.”²⁰ In his speech to the 2003 Network-Centric Warfare Conference, Admiral Cebrowski described the fundamental nature of the NCW concept.

Let’s look at networking ... when we shift from being platform centric to network centric we shift from focusing on things to focusing on behavior or action ... what we are really talking about is a new theory of war because we are talking about new sources of power. The United States Air Force talks about being able to destroy a target using only one bomb where it used to take 1,000 bombs. If you look at the difference between the 1,000 and the one and how it is done the only difference is the [information technology]. You have a 1,000 to one substitution of information for mass.²¹

There is little evidence of anyone challenging the utility of a force, from tactical to strategic, that is able to maintain common situational awareness. The true debate centers on the ability to maintain the network, and what happens to the force that is tailored and thus dependant on said network when battlefield conditions disrupt or deny the networks connectivity.

In 2001, DOD leadership made a fundamental assumption that they would be able to maintain network connectivity as described above, and embarked on a transformation

²⁰ Director, Office of Force Transformation, Office of Secretary of Defense, "Network-Centric Warfare: Creating a Decisive Warfighting Advantage," (Washington, D.C., winter 2003).

²¹ Arthur Cebrowski, "Speech to the Network Centric Warfare 2003 Conference."

plan to adjust the force based on those perceived efficiencies. In what should be an obvious point, Martin Van Creveld notes that “The more centralized the system, the greater the danger that it will be paralyzed if enemy action causes the directing brain to be eliminated or communications with it to be impaired.”²² The centralization concern in this context is not the units on the battlefield, which in fact can be more distributed under NCW, but the reliance of the entire force on network connectivity; i.e. a potential single point of failure at the operational level. However, this point has been largely ignored by defense planners and leadership.

Perhaps acknowledging this reality, the military’s senior strategies show a downward trend in enforcing the precepts of NCW. The 2004 NMS identified eight capability areas that “provide a transformation focus for the Department,”²³ one of which was “Conducting Network-Centric Operations.”²⁴ The 2005 NDS maintained this focus, but with slightly less forceful language, saying “The foundation of our operations proceeds from a simple proposition: the whole of an integrated and networked force is far more capable than the sum of its parts.”²⁵ The 2008 NDS retained the concept, but backed a little further away from its imperatives. “Concepts such as ‘net-centricity’ can help guide DoD ... forging the Total Force into more than the sum of its parts These

²² Martin L. Van Creveld, *Technology and War*, 317.

²³ DOD, *The National Military Strategy*, 23.

²⁴ Ibid.

²⁵ DOD, *The National Defense Strategy*, (2005), 14.

concepts are not a panacea, and will require investments in people as much as in technology to realize the full potential of these initiatives.”²⁶ In line with the 2008 NDS, the 2008 JOE states that:

Communication and information technologies will significantly advance the capabilities of the Joint Force. Nevertheless, those same advances will be available to America’s opponents and they will use [them] to attack, degrade, and disrupt communications and the flow of information ... [it is] essential that joint forces be capable of functioning in an information hostile environment, so as not to create an Achilles’ heel by becoming too network dependent.²⁷

Though its strategic documents back progressively away from NCW ideals, the U.S. armed forces are still feeling the effects of the initial concept.

Information Dominance

As RMA proposed a vision of technical solutions to warfare challenges and NCW was the medium to attain the vision, Information Dominance was the goal of NCW; “network-centric warfare states that technology ... will provide the information superiority that is at the heart of all DOD concepts.”²⁸ Information dominance has many aliases, such as dominant battlefield awareness, the information war, and information superiority; these terms are often interchanged in the references throughout this section.

²⁶ DOD, *The National Defense Strategy*, (2008), 20.

²⁷ United States Joint Forces Command, *The Joint Operating Environment*, 23.

²⁸ Thomas X. Hammes, *The Sling and the Stone*, 8.

According to Ullman and James, “What is most exciting among these [military] revolutions is ...the capability to have near-perfect knowledge and information of the battlefield ... while depriving the adversary of that capacity and producing ‘systems of systems’ for this purpose.” The resulting information dominance would allow the U.S. to apply limited precision assets at key locations in order to win decisively.²⁹

In opposition to this concept, Colonel Hammes says that a discussion of information dominance is like the ancient story of the emperor’s new clothes, “everyone knows there is not much there but is reluctant to address the issue. A genuine discussion of ‘information dominance’ requires trying to understand and predict the complicated, increasingly fragmented, all-too-human real world.”³⁰ Hammes concludes that a bit of self-reflection is in order. “An honest evaluation of our demonstrated inability to achieve information dominance ... might reveal its implausibility, as evidenced by our lack of understanding of the situation in Iraq and Afghanistan and our inability to come to grips with the worldwide al-Qaeda network.”³¹

U.S. information superiority cannot be assumed on the modern battlefield.

Consider the following from author Tom Ricks:

The pre-Iraq, triumphalist U.S. military also was fond of talking about ‘information dominance.’ What this tended to mean in reality was amassing data rather than understanding. For most of the time the U.S.

²⁹ Harlan Ullman and James Wade, Jr., *Shock & Awe*, 4-5, 9.

³⁰ Thomas X. Hammes, *The Sling and the Stone*, 6-7.

³¹ Ibid.

military has been in Iraq, it actually has tended to be information poor American soldiers would really only start getting the requisite amount of information after they moved out into the population in 2007. In retrospect, this seems like common sense. After all, Clausewitz ... notes that the people are the greatest single source of information available. 'We refer not so much to the single outstandingly significant report, but to the countless minor contacts brought about by the daily activities of our army,' he explained.³²

Operation Iraqi Freedom was an information dominance testbed; it did not execute as envisioned.

To those that would attempt to gain near-perfect knowledge of any battlefield situation, Martin Van Creveld wrote that success in war is inconceivable unless the commander is "grounded in an ability to tolerate uncertainty, cope with it, and make use of it."³³ General Mattis said that "The joint force must act in uncertainty and thrive in chaos, sensing opportunity therein and not retreating into a need for more information."³⁴ "Acknowledging the unpredictability of war is fundamental to our view of future conflict."³⁵

As with the preceding sections, this one will close out with an eye towards the future strategic environment.

³² Thomas E. Ricks, *The Gamble, General David Petraeus and the American Military Adventure in Iraq, 2006-2008*, (New York: The Penguin Press, 2009), 163.

³³ Martin L. Van Creveld, *Technology and War*, 316.

³⁴ J.N. Mattis, "Assessment of Effects Based Operations," *Memorandum for U.S. Joint Forces Command*, (Norfolk: DOD, 14 August 2008), 1.

³⁵ J.N. Mattis, "USJFCOM Commander's Guidance for Effects-Based Operations," (Norfolk: DOD, 14 August 2008), 4-5.

Human conflict ... will not change no matter what advances in technology or computing power may occur: fog and friction will distort, cloak, and twist the course of events. Fog will result from information overload, our own misperceptions and faulty assumptions, and the fact that the enemy will act in an unexpected fashion. Combined with the fog of war will be its frictions - that almost infinite number of seemingly insignificant incidents and actions that can go wrong, the impact of chance, and the horrific effect of combat on human perceptions Although many pundits have touted the ability of information to “lift the fog and friction of war,” such claims have foundered on the rocks of reality.³⁶

The continual struggle for accurate information of the battlefield is every commander’s duty and it would be criminal for DOD leaders not to do everything in their power to support this end. However, the department would be better served to train its leaders to thrive in chaos in addition to equipping the force in such a way that it can continue to function in the same chaotic environment.

³⁶ United States Joint Forces Command, *The Joint Operating Environment*, 5, 22.

APPENDIX C

AIR/SPACE-BASED SYSTEM CAPABILITIES

This Appendix provides specific system configuration and capabilities data for the equipment addressed in Chapter 2.

MQ-1 Predator

The most common sensor configuration based on published technological systems is the Raytheon AN/AAS-52 MTS-A, or the L3 Wescam 14TS.¹ Both systems have an Electro-optical (daylight) TV camera, an Infra-red (thermal) camera, as well as a laser illuminator/range finder; the system can operate one camera at a time. While actual parameters used on U.S. systems remain classified due to physical and software enhancements, they generally have up to seven field of view (FOV) selections, from .21° to 45° with the image resolution increasing as the FOV narrows; up to a maximum 10:1 digital zoom.²

¹ Jane's, *Unmanned Aerial Vehicles and Targets*, Unmanned Aerial Vehicles/GA-ASI MQ-1B and RQ-1A Predator; Payloads/Raytheon AN/AAS-52 MTS-A; Payloads/L-3 Wescam 14TS.

² Ibid., Unmanned Aerial Vehicles/GA-ASI MQ-1B and RQ-1A Predator; Payloads/Raytheon AN/AAS-52 MTS-A; Payloads/L-3 Wescam 14TS; GlobalSecurity.org, *Military, Systems, Aircraft*, UAV/MQ-1B Predator.

Sensors	- Color nose camera for flight control - Electro-optical TV camera - Infra-red camera
C2	- CONUS-based - can launch/recover forward with deployed assets
Communications	Satellite and line-of-sight data links
Launch/Recovery	6000 ft hard surface runway
Endurance	12-24 hours
Range	454 miles
Ceiling	25,000 feet
Qty on hand	138 as of FY09 (plus 12 MQ-1C)
Cost	\$20 million per system



Table 1: MQ-1 Predator (U.S. Army MQ-1C Sky Warrior)³

MQ-9 Reaper

Sensor capabilities are represented by the Raytheon AN/DAS-1 MTS-B, which improves the range of the EO/IR cameras in the MTS-A discussed in the Predator sensor package, and adds an additional image-intensifying TV camera.⁴ The Reapers' GTMI/SAR capability is best represented by the GA-ASI AN/APY-8 Lynx Block 20/25.⁵ The SAR has both strip and spotlight FOV options between 45°-135° at a slant range⁶ of

³ GlobalSecurity.org, *Military, Systems, Aircraft, UAV/MQ-1B Predator*; Greg Goebel, *In the Public Domain, Unmanned Aerial Vehicles*, 1 February 2010, available from <http://www.vectorsite.net/twuav.html>; Internet; accessed 13 February 2010: [13.0] Modern US Endurance UAVs; Jane's, *Unmanned Aerial Vehicles and Targets*, Unmanned Aerial Vehicles/GA-ASI MQ-1B and RQ-1A Predator; Payloads/Raytheon AN/AAS-52 MTS-A; Payloads/L-3 Wescam 14TS; U.S. Air Force, *Factsheets*, MQ-1 Predator.

⁴ Jane's, *Unmanned Aerial Vehicles and Targets*, Unmanned Aerial Vehicles/GA-ASI MQ-9 Reaper, Predator B and Mariner; Payloads/Raytheon AN/DAS-1 MTS-B.

⁵ Ibid., *Unmanned Aerial Vehicles/GA-ASI MQ-9 Reaper, Predator B and Mariner*; Payloads/GA-ASI AN/APY-8 Lynx Block 20/25.

⁶ Slant range is the maximum allowable straight-line distance between the aircraft and the target where the aircraft can maintain desired imagery resolution. Assuming a maximum aircraft ceiling capacity, slant

50 miles in order maintain 3 meter resolution, and 18.6 miles for a classified “high resolution.”⁷ The GTMI retains the same slant range as the SAR, but operates with a 135° FOV.

Sensors	<ul style="list-style-type: none"> - Color nose camera for flight control - Electro-optical TV camera - Image-intensified TV camera - Infra-red camera - Synthetic Aperture Radar/Ground Moving Target Indicator
C2	CONUS-based
Communications	Satellite and line-of-sight data links
Launch/Recovery	standard U.S. airfields
Endurance	12-32 hours
Range	4600-5300 miles
Ceiling	50,000 feet
Qty on hand	10 as of FY09
Cost	\$57 Million per system (FY09 Dollars)



Table 2: MQ-9 Reaper⁸

range is irrespective of the aircraft's elevation until it descends to a point where either terrain or the curvature of the earth obscures observation of the target.

⁷ Ibid., Payloads/GA-ASI AN/APY-8 Lynx Block 20/25.

⁸ Greg Goebel, *In the Public Domain, Unmanned Aerial Vehicles*, [13.0] Modern US Endurance UAVs; GlobalSecurity.org, *Military, Systems, Aircraft*, UAV/MQ-9B Reaper; Jane's, *Unmanned Aerial Vehicles and Targets*, Unmanned Aerial Vehicles/GA-ASI MQ-9 Reaper, Predator B and Mariner; Payloads/Raytheon AN/DAS-1 MTS-B; Payloads/GA-ASI AN/APY-8 Lynx Block 20/25; National Aeronautics and Space Administration, *Dryden Flight Research Center Factsheets*, 9 July 2009, available from <http://www.nasa.gov/centers/dryden/news/FactSheets/alphabetized.html>; Internet; accessed 13 February 2010: Altair/Predator B; U.S. Air Force, *Factsheets*, MQ-9 Reaper.

RQ-4 Global Hawk

The Global Hawk carries a variant of either the Hughes Integrated Surveillance and Reconnaissance (HISAR) sensor suite, or the Raytheon Enhanced Integrated Sensor Suite (EISS); both systems have an EO/IR camera and SAR/GMTI.⁹ The EO/IR camera is capable of resolution down to 3 feet.¹⁰ The SAR/GMTI retains the multiple mode settings of earlier systems but with significantly greater capabilities. The SAR spot mode can provide 6 foot resolution over 3.8 square miles, the combined SAR-GMTI strip mode provides 20 foot resolution for a 23 mile wide by 12-68 mile long strip, and the wide-area GMTI mode can detect moving targets within a radius of 62 miles.¹¹ The Global Hawk is slated to upgrade its sensor package to the Northrop Grumman/Raytheon Multi-Platform Radar Technology Insertion Program (MP-RTIP).¹² Though the particulars remain classified, it is reportedly capable of one foot resolution at the current slant range.¹³

⁹ Greg Goebel, *In the Public Domain, Unmanned Aerial Vehicles*, [13.0] Modern US Endurance UAVs.

¹⁰ GlobalSecurity.org, *Military, Systems, Aircraft*, UAV/RQ-4 Global Hawk.

¹¹ Greg Goebel, *In the Public Domain, Unmanned Aerial Vehicles*, [13.0] Modern US Endurance UAVs.

¹² Jane's, *Unmanned Aerial Vehicles and Targets*, Unmanned Aerial Vehicles/Northrop Grumman RQ-4 Global Hawk.

¹³ GlobalSecurity.org, *Military, Systems, Aircraft*, UAV/RQ-4 Global Hawk.

Sensors	- Electro-optical TV camera - Infra-red camera - Synthetic Aperture Radar/Ground Moving Target Indicator or - future SIGINT package
C2	CONUS-based
Communications	Satellite and line-of-sight data links
Launch/Recovery	5000 ft minimum runway
Endurance	30-42 hours
Range	10,000-11,000 miles
Ceiling	60,000 feet
Qty on hand	- USAF has 10 as of FY09 - USN purchasing unpublished amount starting in FY12
Cost	\$39.5-84 Million per system (FY09 Dollars)



Table 3: RQ-4 Global Hawk (U.S. Navy RQ-4N)¹⁴

MC-12 Liberty

The most probable sensor system is the L-3 Wescam MX-15i electro-optical camera. The system produces full motion video using one of two daylight cameras or an infra-red camera. Together the three camera settings provide FOV options from .43° to 31.8°, with a maximum x19 zoom.¹⁵

¹⁴ Greg Goebel, *In the Public Domain, Unmanned Aerial Vehicles*, [13.0] Modern US Endurance UAVs; GlobalSecurity.org, *Military, Systems, Aircraft*, UAV/RQ-4 Global Hawk; Jane's, *Unmanned Aerial Vehicles and Targets*, Unmanned Aerial Vehicles/Northrop Grumman RQ-4 Global Hawk; National Aeronautics and Space Administration, *Dryden Flight Research Center Factsheets*, Global Hawk; U.S. Air Force, *Factsheets*, RQ-4 Global Hawk. The U.S. Navy is purchasing the systems in support of its Broad Area Maritime Surveillance (BAMS) program, a plan to maintain UAV coverage over key maritime chokepoints and sea lines of communication. For more information see the STRATFOR Global Intelligence assessment of BAMS at

http://www.stratfor.com/analysis/united_states_broad_area_maritime_surveillance.

¹⁵ Jane's, *Unmanned Aerial Vehicles and Targets*, Payloads/MX-15.


Sensors	- Electro-optical TV camera - Infra-red camera	
Communications	Satellite and line-of-sight voice and data links	
Endurance	greater than 8 hours	
Range	1500 or 2400 miles	
Ceiling	35,000 feet	
Qty on hand	29 as of FY09; 37 planned (MARRS may have 18 more)	
Cost	\$17 Million (FY09 Dollars)	

Table 4: MC-12 Liberty (U.S. Army MARSS)¹⁶

RC-135V/W Rivet Joint

The current sensor package is known as the 85000 COMINT suite, and its primary component is the E-Systems ES182 Multiple Communication Emitter Location System (MUCELS).¹⁷ While the specifics of both the sensor package and the supporting communications backbone remain classified, it is reportedly capable of ELINT and COMINT intercept operations against targets at ranges of up to 150 miles;¹⁸ perhaps being able to monitor targets ranging from cell phones to air defense radars.¹⁹ The Rivet Joint package is believed to have direction finding limitations in emerging high frequency systems. In addition, employment remains challenged due to the maximum 120° sensor FOV on either side of the aircraft; one side at a time.²⁰

¹⁶ GlobalSecurity.org, *Military, Systems, Aircraft*, RC-12/MC-12 Liberty; U.S. Air Force, *Factsheets*, MC-12; Jane's, *All the World's Aircraft*, Hawker Beechcraft King Air 300/350 series/MC-12W surveillance variants.

¹⁷ Jane's, *All the World's Aircraft*, Boeing RC-135U/V/W.

¹⁸ GlobalSecurity.org, *Military, Systems, Aircraft*, RC-135.

¹⁹ Jane's, *All the World's Aircraft*, Boeing RC-135U/V/W.

²⁰ GlobalSecurity.org, *Military, Systems, Aircraft*, RC-135.


Sensors	- Communications Intelligence - Electronic Intelligence	
Communications	Satellite and line-of-sight voice and data links	
Endurance	11 hours (20 with aerial refuel)	
Range	3900 miles without aerial refuel	
Ceiling	50,000 feet	
Qty on hand	17 (FY09)	
Cost	Unknown	

Table 5: RC-135V/W Rivet Joint²¹

E-8C JSTARS

The E-8C currently uses the Northrop Grumman AN/APY-3 multimode side-looking phased-array radar. The radar is mounted underneath the aircraft and provides a 120° FOV that can monitor one side of the aircraft at a time; it can shift sides as needed.²² The system has two operating modes: Wide Area Surveillance/Moving Target Indicator (WAS/MTI) and Synthetic Aperture Radar/Fixed Target Indicator (SAR/FTI). Operating primarily in WAS/MTI, the system is able to locate slow-moving ground targets up to 150 miles from the aircraft then switch to SAR/FTI to create radar imagery of stationary assets.²³ The sensor package is upgrading to the currently classified MP-RTIP discussed above for the Global Hawk, reportedly capable of 12-14 foot resolution.²⁴

²¹ GlobalSecurity.org, *Military, Systems, Aircraft*, RC-135; Jane's, *All the World's Aircraft*, Boeing RC-135U/V/W; U.S. Air Force, *Factsheets*, RC-135V/W RIVET JOINT.

²² Jane's, *All the World's Aircraft*, Northrop Grumman E-8 Joint Stars.

²³ GlobalSecurity.org, *Military, Systems, Aircraft*, E8.

²⁴ Ibid.

Sensors	Multimode side-looking phased-array I-band radar: - Wide Area Surveillance/Moving Target Indicator - Synthetic Aperture Radar/Fixed Target Indicator
Communications	Satellite and line-of-sight voice and data links
Endurance	9-11 hours (20 with aerial refuel)
Range	5800 miles
Ceiling	42,000 feet
Qty on hand	17
Cost	\$318 Million (FY09 Dollars)



Table 6: E8C Joint Surveillance Target Attack Radar System (JSTARS)²⁵

U2S Dragon Lady

Though actual parameters are classified, the U2's IMINT capabilities are represented by the Itek SENIOR YEAR Electro-optical Reconnaissance System (SYERS), the Raytheon Advanced Synthetic Aperture Radar System (ASARS-2A), and the Itek 30 inch focal length optical bar camera (OBC)²⁶; the OBC produces traditional film products for exploitation after landing.²⁷ The SYERS EO/IR camera system provides a 75 mile range compared to the ASARS-2A with a 112 mile range.²⁸ Specifically, the ASARS-2A has a moving target indicator mode capable of 3 foot resolution for a swathe 3 miles wide, a fixed target indicator mode capable of 10 foot resolution for a swathe 115 miles wide, and a spotlight mode capable of 1 foot resolution

²⁵ GlobalSecurity.org, *Military, Systems, Aircraft*, E8; Jane's, *All the World's Aircraft*, Northrop Grumman E-8 Joint Stars; U.S. Air Force, *Factsheets*, E-8C JOINT STARS.

²⁶ Jane's, *All the World's Aircraft*, Lockheed Martin U-2S.

²⁷ U.S. Air Force, *Factsheets*, U-2S/TU-2S.

²⁸ GlobalSecurity.org, *Military, Systems, Aircraft*, SENIOR YEAR / AQUATONE / U-2 / TR-1.

for 1 square mile.²⁹ The U2S also provides a SIGINT package of both electronics intelligence (ELINT) and communications intelligence (COMINT) capable of interception and monitoring at 174 mile range.³⁰

Sensors	- Electro-optical/Infra-red camera - Synthetic Aperture Radar/Moving Target Indicator - Optical Bar camera - SIGINT package
Communications	Satellite and line-of-sight voice and data links
Endurance	12 hours
Range	7000+ miles
Ceiling	90,000 feet
Qty on hand	26 (2 more at NASA)
Cost	Classified



Table 7: U2S Dragon Lady³¹

Improved Crystal

Its sensors operate in visible light, near IR, and thermal IR; capable of a resolution near 4 inches at a high slant angle.³² Selected sources suggest that a KH-13 system is under development that incorporates a radar package and an improved IR system capable of 1.6 inch resolution.³³

²⁹ Jane's, *Unmanned Aerial Vehicles and Targets*, Payloads/ASARS-2 Advanced Synthetic Aperture Radar System.

³⁰ GlobalSecurity.org, *Military, Systems, Aircraft*, SENIOR YEAR / AQUATONE / U-2 / TR-1.

³¹ GlobalSecurity.org, *Military, Systems, Aircraft*, SENIOR YEAR / AQUATONE / U-2 / TR-1; Jane's, *All the World's Aircraft*, Lockheed Martin U-2S; Jane's, *Unmanned Aerial Vehicles and Targets*, Payloads/ASARS-2 Advanced Synthetic Aperture Radar System; U.S. Air Force, *Factsheets*, U-2S/TU-2S.

³² GlobalSecurity.org, *Space Menu, Systems*, Imagery Intelligence/KH-12 Improved Crystal.

³³ T.W. Lee, *Military Technologies of the World*, 146.

Sensors	Opical and Infra-red
Communications	Relay through Milstar communications satellites
Lifespan	5-9 years
Orbit	Low Earth Orbit
Qty on hand	2 satellites (2-3 older/degraded are still in space)
Cost	approximately \$1.7 billion including the launch vehicle

Table 8: Improved/Advanced Crystal, IKON, or KH-12³⁴

Lacrosse

The radar is believed capable of resolutions between 2-3 feet,³⁵ but this resolution limits coverage down to a few square miles. While this is much less than the Advanced Crystal optical resolution, it is sufficient for identification of larger military vehicles and installations. The Lacrosse probably uses a number of scanning modes with lower resolutions able to cover hundreds of square miles. The newest Lacrosse satellite is believed to maintain operational capability through 2012.³⁶

Sensors	Infra-red and Phased array rader
Communications	Relay through Milstar communications satellites
Lifespan	5-7 years
Orbit	Low Earth Orbit
Qty on hand	2-3 satellites (possibly 2 more older/degraded still in space)
Cost	approximately \$1.4 billion including the launch vehicle

Table 9: Lacrosse, Onyx, Vega³⁷

³⁴ GlobalSecurity.org, *Space Menu, Systems*, Imagery Intelligence/KH-12 Improved Crystal; Jane's, *Space Systems and Industry*, Improved Crystal.

³⁵ Jane's, *Space Systems and Industry*, Lacrosse/Onyx series.

³⁶ GlobalSecurity.org, *Space Menu, Systems*, Imagery Intelligence/Lacrosse/Onyx.

³⁷ Ibid.; Jane's, *Space Systems and Industry*, Lacrosse/Onyx series.

Mentor

Lifespan	8-12 years
Orbit	Geosynchronous Orbit
Qty on hand	3 satellites (possibly 2 more older/degraded still in space)
Cost	greater than \$2 billion including the launch vehicle

Table 10: Mentor, Advanced Mentor, Advanced Orion³⁸

Trumpet

Lifespan	8-12 years
Orbit	Highly Elliptical Orbit (23K x ~200 miles at 63° inclination)
Qty on hand	3 satellites
Cost	approximately \$1.3 billion including the launch vehicle

Table 11: Trumpet³⁹

Mercury

Lifespan	8-12 years
Orbit	Geosynchronous orbit
Qty on hand	2 satellites
Cost	greater than \$500 million including the launch vehicle

Table 12: Mercury, Vortex-II, Advanced Vortex⁴⁰

³⁸ GlobalSecurity.org, *Space Menu, Systems*, Mentor; Jane's, *Space Systems and Industry*, SIGINT.

³⁹ GlobalSecurity.org, *Space Menu, Systems*, Mentor; Jane's, *Space Systems and Industry*, Trumpet Series.

⁴⁰ GlobalSecurity.org, *Space Menu, Systems*, Signals Intelligence/Mercury; Jane's, *Space Systems and Industry*, SIGINT.

BIBLIOGRAPHY

- Alexander, Keith B. "Warfighting in Cyberspace." *Joint Forces Quarterly*, no. 46 (3rd Quarter 2007): 58-61.
- Boot, Max. *The Savage Wars of Peace: Small Wars and the Rise of American Power*. New York: Basic Books, 2002.
- Bush, George W. "The National Security Strategy of the United States of America." Washington, D.C.: The White House, 2006.
- Cebrowski, Arthur. "Speech to the Network Centric Warfare 2003 Conference." *Center for Defense Information, Military Reform Project*. <http://www.cdi.org/mrp/tt-17feb03.pdf> (accessed October 15, 2009).
- . "Transforming Transformation." *Transformation Trends*. Arlington: Office of Force Transformation, April 19, 2004.
- Department of Defense. "Defense Intelligence Strategy." Washington, D.C., 2008.
- . *Joint Publication 1, Doctrine for the Armed Forces of the United States*. Washington, D.C., 2009.
- . *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms*. Washington, D.C., 2009.
- . *Joint Publication 2-0, Joint Intelligence*. Washington, D.C., 2007.
- . *Joint Publication 2-01, Joint and National Intelligence Support to Military Operations*. Washington, D.C., 2004.
- . *Joint Publication 3-0, Joint Operations*. Washington, D.C., 2008.
- . *Joint Publication 5-0, Joint Operation Planning*. Washington, D.C., 2006.
- Department of Defense. "Military Power of the People's Republic of China, 2009." Annual Report to Congress, Washington, D.C., 2009.
- Department of Defense. "Quadrennial Defense Review Report." Washington, D.C., 2006.

- Department of Defense. "The National Defense Strategy." Washington, D.C., 2008.
- Department of Defense. "The National Defense Strategy of the United States of America." Washington, D.C., 2005.
- Department of Defense. "The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow." Washington, D.C., 2004.
- Department of Defense. "Transformation Planning Guidance." Washington, D.C., 2003.
- Deptula, David A, and James R Marrs. "Global Distributed ISR Operations: The Changing Face of Warfare." *Joint Forces Quarterly*, no. 54 (3rd Quarter 2009): 110-115.
- Director, Office of Force Transformation, Office of Secretary of Defense. "Network-Centric Warfare: Creating a Decisive Warfighting Advantage." Washington, D.C., winter 2003.
- Dolman, Everett C. "A Debate About Weapons in Space: For U.S. Military Transformation and Weapons in Space." *SAIS Review*, 2006: 163-174.
- Friedman, Norman. *Terrorism, Afghanistan, and America's New Way of War*. Annapolis: Naval Institute Press, 2003.
- GlobalSecurity.org. *Military, Systems, Aircraft*. December 14, 2009.
<http://www.globalsecurity.org/military/systems/aircraft/index.html> (accessed February 13, 2010).
- . *Space Menu, Systems*. December 14, 2009.
<http://www.globalsecurity.org/space/systems/index.html> (accessed February 28, 2010).
- Goebel, Greg. *In the Public Domain, Unmanned Aerial Vehicles*. February 1, 2010.
<http://www.vectorsite.net/twuav.html> (accessed February 13, 2010).
- Gordon, Michael R., and Bernard E. Trainor. *COBRA II: The Inside Story of the Invasion and the Occupation of Iraq*. New York: Pantheon Books, 2006.
- Gray, Colin S. "Why Strategy is Difficult." *Joint Forces Quarterly*, no. 22 (Summer 1999): 6-12.

- Hammes, Thomas X. *The Sling and the Stone: On War in the 21st Century*. St. Paul: Zenith Press, 2006.
- Headquarters, Department of the Army. *Field Manual 3-90, Tactics*. Washington, D.C., 2001.
- Howcroft, James R. "Technology, Intelligence, and Trust." *Joint Forces Quarterly*, no. 46 (3rd Quarter 2007): 20-26.
- Ignatieff, Michael. *Virtual War, Kosovo and Beyond*. New York: Picador USA, 2000.
- Jane's. *all the world's aircraft*. February 2010, 10.
http://jawa.janes.com/docs/jawa/browse_section_results.jsp?SelPub=jawa&bucket=Section&selected=AIRCRAFT+-+FIXED-WING+-+MILITARY&sort=Country-false&pageCount=-1 (accessed February 16, 2010).
- . *space systems and industry*. February 10, 2010.
http://jsd.janes.com/docs/jsd/browse_section_results.jsp?SelPub=jsd&bucket=Section&selected=SPACECRAFT+-+DEFENCE&sort=Country-false&pageCount=-1 (accessed March 1, 2010).
- . *unmanned aerial vehicles and targets*. February 10, 2010.
http://juav.janes.com/docs/juav/browse_section.html (accessed February 13, 2010).
- Kostka, Del C. "Moving Toward a Joint Acquisition Process to Support ISR." *Joint Forces Quarterly*, no. 55 (4th Quarter 2009): 69-75.
- Lee, T.W. *Military Technologies of the World*. Westport, CT: Praeger Security International, 2009.
- Mattis, J. N. "Assessment of Effects Based Operations." *Memorandum for U.S. Joint Forces Command*. Norfolk: Department of Defense, August 14, 2008.
- . "USJFCOM Commander's Guidance for Effects-Based Operations." Norfolk: Department of Defense, August 14, 2008.
- McConnell, Mike. "Overhauling Intelligence." *Foreign Affairs*, July/August 2007: 49-58.
- McElroy, Robert H. "Afghanistan, Fire Support for Operation Anaconda." *Field Artillery*, September/October 2002: 5-9.

- Melshen, Paul. "Mapping Out a Counterinsurgency Plan: Critical Considerations in Counterinsurgency Campaigning." *Small Wars and Insurgencies* 18, no. 4 (December 2007): 665-698.
- National Aeronautics and Space Administration. *Dryden Flight Research Center Factsheets*. July 9, 2009.
<http://www.nasa.gov/centers/dryden/news/FactSheets/alphabetized.html> (accessed February 13, 2010).
- National Aeronautics and Space Administration, Global Change Master Directory. *Ancillary Description Writer's Guide*. 2008.
<http://gcmd.nasa.gov/User/suppguide/platforms/orbit.html> (accessed February 4, 2010).
- Odierno, Raymond T, Nichoel E Brooks, and Francesco P Mastracchio. "ISR Evolution in the Iraqi Theater." *Joint Forces Quarterly*, no. 50 (3rd Quarter 2008): 51-55.
- Peters, Ralph. "The Counterrevolution in Military Affairs: Fashionable Thinking about Defense Technology Ignores the Great Threats of Our Time." *The Weekly Standard*, February 6, 2006: 18-24.
- Petraeus, David H. *Multinational Force-Iraq Counterinsurgency Guidance*. June 6, 2007.
http://www.airforce.forces.gc.ca/CFAWC/Contemporary_Studies/2007/2007-Jun/2007-06-06_MNF-I_COIN_Guidance-Summer_2007_v7_e.asp (accessed October 6, 2009).
- Record, Jeffery. *The Creeping Irrelevance of U.S. Force Planning*. Monograph, Carlisle Barracks: Strategic Studies Institute, U.S. Army War College, 1998.
- Ricks, Thomas E. *The Gamble, General David Petraeus and the American Military Adventure in Iraq, 2006-2008*. New York: The Penguin Press, 2009.
- Risen, Clay. "War-Mart: the danger of generals-as-CEOs." *The New Republic*, April 3, 2006: 20.
- Romjue, John L. *From Active Defense to AirLand Battle: The Development of Army Doctrine, 1973-1982*. Fort Monroe: Historical Office, United States Army Training and Doctrine Command, 1984.
- Shanker, Thom, and Eric Schmitt. *The New York Times*. February 24, 2010.
<http://query.nytimes.com/gst/fullpage.html?res=9C07E2DD143CF937A15751C0A9669D8B63&scp=5&sq=thom+shanker&st=nyt> (accessed March 3, 2010).

- STRATFOR Global Intelligence. *Military/Tracking U.S. Naval Power*. April 23, 2008.
http://www.stratfor.com/analysis/united_states_broad_area_maritime_surveillance
 e (accessed February 13, 2010).
- Tarr, David W. *American Strategy in the Nuclear Age*. New York: Macmillan Publishing Co., Inc, 1966.
- Tzu, Sun. *The Art of War*. Translated by Samuel B. Griffith. London: Oxford University Press, 1963.
- U.S. Air Force. *Factsheets*. <http://www.af.mil/information/factsheets/> (accessed February 9, 2010).
- Ullman, Harlan, and James Jr Wade. *Shock & Awe: Achieving Rapid Dominance*. Washington, D.C.: U.S. Government Printing Office, 1996.
- United States Army. *The Official Webpage of the United States Army*. March 1, 2010.
<http://www.army.mil/info/organization/> (accessed March 9, 2010).
- United States Government Accountability Office. *Intelligence, Surveillance, and Reconnaissance: DOD Can Better Assess and Integrate ISR Capabilities and Oversee Development of Future ISR Requirements*. Report to the Subcommittee on Air and Land Forces, Committee on Armed Services, House of Representatives, Washington, D.C.: USGAO, 2008.
- United States Government Accountability Office. *Intelligence, Surveillance, and Reconnaissance: Preliminary Observations on DOD's Approach to Managing Requirements for New Systems, Existing Assets, and Systems Development*. Testimony before the Subcommittee on Air and Land Forces, Committee on Armed Services, House of Representatives, Washington, D.C.: USGAO, 2007.
- United States Joint Forces Command. "The Joint Operating Environment: Challenges and Implications for the Future Joint Force." Suffolk, VA, 2008.
- United States Special Operations Command Public Affairs. *USSOCOM Fact Book*. March 5, 2010.
<http://www.socom.mil/SOCOMHome/newspub/pubs/Documents/FactBook.pdf>
 (accessed March 7, 2010).
- USMC Program Assessment and Evaluation Division. *Concepts and Programs*. Washington, D.C.: DMA Marine Corps, 2009.

Van Creveld, Martin L. *Technology and War: From 2000 B.C. to the Present*. New York: The Free Press, 1991.

War Department. *Report of the Secretary of War to the President*. Annual, Washington D.C.: United States Government Printing Office, 1933.

Wong, Wilson W.S., and James Fergusson. *Military Space Power: A Guide to the Issues*. Santa Barbara, CA: ABC-CLIO, LLC, 2010.

VITA

Major Glen E. Clubb, U.S. Army, is an Armored Cavalry Officer and currently a Graduate Student at the Joint Advanced Warfighting School. He has deployed operationally in an Armored Cavalry Regiment, a Divisional Cavalry Squadron, and a Brigade Armored Reconnaissance Squadron.

